SOME RECENT INVESTIGATIONS CONCERNING THE SECTIONS OF POWER SERIES AND RELATED DEVELOPMENTS*

BY GABRIEL SZEGÖ

1. *Introduction.* The definition of analytic functions given by Weierstrass is based primarily on the notion of power series. Numerous results and questions of the modern theory of these functions can be formulated as definite relations between the coefficients of a power series and the values of the corresponding function inside or outside of the circle of convergence or on this circle itself. Analogous questions may be raised concerning trigonometric series. In what follows a short report of some recent investigations in this direction will be given. The vastness of this field makes it impossible to be complete. Thus we point out mainly the typical methods used and the most characteristic results.†

2. *Problem.* We consider the set or the class of power series

$$c_0 + c_1 z + c_2 z^2 + \cdots + c_n z^n + \cdots \tag{1}$$

convergent in a circle of the complex z plane (say for $|z| < 1$) and satisfying some conditions there, say C. In a very general formulation the problem is to find necessary and sufficient conditions in terms of the coefficients c_n in order that the function $f(z)$ represented by (1) should satisfy the condition C. This problem has been solved in a more or less applicable form only for some special classes of power series. In 1911 Carathéodory [1] and Toeplitz [39] obtained a condition of this kind for power series $f(z)$ with a positive real part in the unit circle. Their condition has a "quasi-algebraic" character, containing an infinite number of algebraic conditions. A second very important class, that of power series remaining bounded in the unit circle, $|f(z)| \leq M$, can be reduced, at least in principle, to the class mentioned

* An address delivered at the meeting of the Society on January 1, 1936, in St. Louis, by invitation of the Program Committee.

† Some of the older results referred to in this paper are contained in a previous report on this subject. See [34] in the list of references given at the end of the paper.

[Carathéodory and Fejér, 2]. This reduction gives a possibility of characterizing the boundedness property again by some conditions in terms of the coefficients. In 1917 Schur [27] gave a very elegant algebraic form for these conditions.

Apart from these special classes and some other classes more or less connected with them, it is rather hopeless to expect an exhaustive solution of this problem. For instance, we do not know the necessary and sufficient conditions in terms of the coefficients in order that $f(z)$ should be a simple or univalent function in the unit circle. Therefore we confine ourselves to a more special question asking for some properties of the coefficients c_n or of the terms $c_n z^n$ of the power series (1), or more generally of some linear combinations of these terms which are implied by the condition C in question. This problem is not at all trivial even for the classes mentioned before. In principle the algebraic characterization of the coefficients yields, of course, a method of attacking the problem; this, however, only in principle, and the effective determination of some maxima or minima connected with the coefficients can be an extremely difficult algebraic task.

It should be emphasized that historically these problems have originated in some questions concerning ordinary Fourier series. It suffices to mention only two questions of this sort which have become rather classical nowadays. The first is the problem of Lebesgue, to determine the maximum of the nth section of the Fourier series of all functions remaining $\leqq 1$ in absolute value.* These maxima, called Lebesgue constants, gained a particular importance through the investigations of Lebesgue, showing that the unboundedness of these constants is the deeper cause of the existence of continuous functions with divergent Fourier series. Another question is Carathéodory's problem of characterizing the Fourier constants of a positive real function, a problem closely related to that mentioned above regarding analytic functions with a positive real part in the unit circle.

3. Bounded Functions. Coefficients, Partial Sums, and Cesàro

* H. Lebesgue, *Sur la divergence et la convergence non-uniforme des séries de Fourier*, Comptes Rendus, vol. 141 (1905), pp. 875–877; *Leçons sur les Séries Trigonométriques*, (1906), art. 45, 46, pp. 86–88. See also A. Haar, *Zur Theorie der orthogonalen Funktionensysteme*, Mathematische Annalen, vol. 69 (1910), pp. 331–371.

Means. Returning to the complex problem, let us consider in a more detailed way the set of power series $f(z)$ satisfying the special condition E: $|f(z)| \leqq 1$ in $|z| < 1$. For the sake of convenience we choose for the upper bound $M = 1$. Cauchy's integral representation of the coefficients furnishes, then, the inequalities $|c_n| \leqq 1$ for all values of n. The bound 1 is of course the best possible since $f(z) = 1$ satisfies condition E. Much more holds, however, namely, that the sum

$$|c_0|^2 + |c_1|^2 + |c_2|^2 + \cdots + |c_n|^2 + \cdots \tag{2}$$

is convergent and also $\leqq 1$. This incidentally is the case for a more extensive class of power series, namely, for the functions $f(z)$ regular in $|z| < 1$ and satisfying there the condition

$$\frac{1}{2\pi}\int_{-\pi}^{+\pi} |f(re^{i\phi})|^2 d\phi \leqq 1, \qquad (r < 1). \tag{3}$$

We return to this class and to related classes in §11.

So much about the limitation of the coefficients or, what is the same, of the single terms. The question arises now what can be said about the partial sums or sections

$$s_n(z) = c_0 + c_1 z + c_2 z^2 + \cdots + c_n z^n \tag{4}$$

of a power series of class E if $|z| \leqq 1$.

The exact maximum of $|s_n(z)|$ in $|z| \leqq 1$ uniformly for the whole class E was determined by Landau [16] in the explicit form

$$1 + \sum_{\nu=1}^{n} \left(\frac{1 \cdot 3 \cdots (2\nu - 1)}{2 \cdot 4 \cdots 2\nu}\right)^2. \tag{5}$$

This expression becomes ∞ for $n \to \infty$, a fact which is in close relation to a previous result of Fejér [5], stating the existence of functions with the property E whose partial sums are *unbounded* in $|z| < 1$. In particular, if $f(z)$ has the property E in $|z| < 1$, the partial sums do not have the same property necessarily in $|z| < 1$.

These results suggest the question of determining the exact maximum or, at any rate, proper upper bounds for a given linear combination

$$L_n(z) = \lambda_0 c_0 + \lambda_1 (c_1 z) + \lambda_2 (c_2 z^2) + \cdots + \lambda_n (c_n z^n) \tag{6}$$

of the first $n+1$ terms of a function $f(z)$ of class E; here z ranges over the unit circle, $|z| \leqq 1$. A very important linear combination of this kind has been pointed out by Fejér [6], who proved that the Cesàro means of (1) satisfy the same condition E as the function itself. Denoting these means by $\sigma_n(z)$, we have

$$\sigma_n(z) = \frac{s_0(z) + s_1(z) + s_2(z) + \cdots + s_n(z)}{n+1} = \frac{S_n(z)}{n+1}$$

$$= \sum_{\nu=0}^{n} \left(1 - \frac{\nu}{n+1}\right) c_\nu z^\nu, \tag{7}$$

and the inequalities $|\sigma_n(z)| \leqq 1$ hold for $|z| \leqq 1$, $(n = 0, 1, 2, \cdots)$. This result has, also, a parallel in the theory of Fourier series. It reminds us of the analogous, nowadays classical, property of the Cesàro means of Fourier series likewise due to Fejér.* The converse of the theorem is also true: The function $f(z)$ has the property E in $|z| < 1$, if and only if the same is valid for *all* the Cesàro means $\sigma_n(z)$ in $|z| \leqq 1$.

4. *Continuation. Linear Combinations.* Various methods have been developed in order to obtain proper upper bounds for the linear combination $L_n(z)$ in (6) if $f(z)$ is in E and $|z| \leqq 1$.

(a) Landau's method was extended by Szász [31], giving an upper bound for $L_n(z)$ in each case, and even obtaining the exact maximum if a certain algebraic condition is satisfied. Assuming $\lambda_n \neq 0$ we develop the expression

$$(\lambda_n + \lambda_{n-1}x + \lambda_{n-2}x^2 + \cdots + \lambda_0 x^n)^{1/2}$$

(with an arbitrary determination of the square root) in a power series $\mu_0 + \mu_1 x + \mu_2 x^2 + \cdots$; the finite sum

$$|\mu_0|^2 + |\mu_1|^2 + |\mu_2|^2 + \cdots + |\mu_n|^2$$

then furnishes the upper bound mentioned. In the particular case when the polynomial $\mu_0 + \mu_1 z + \cdots + \mu_n z^n$ is different from 0 in $|z| < 1$, this is the *exact* maximum in question.

From this general theorem Landau's result $(\lambda_\nu = 1)$ and Fejér's result $(\lambda_\nu = 1 - \nu/(n+1))$ can be easily obtained.

(b) In a joint investigation with Schur [29], we gave an-

* *Untersuchungen über Fouriersche Reihen*, Mathematische Annalen, vol. 58 (1904), pp. 51–69; especially p. 60.

other method, in principle very elementary, of obtaining linear combinations (6) remaining $\leqq 1$ in $|z| \leqq 1$, that is, having the same property E as the function itself. This is, namely, the case if the coefficients λ_ν are real, $\lambda_0 = 1$, and the trigonometric polynomial

$$(8) \qquad T(\phi) = \frac{1}{2} + \lambda_1 \cos\phi + \lambda_2 \cos 2\phi + \cdots + \lambda_n \cos n\phi$$

assumes only non-negative values for all real values of ϕ. This follows readily from the representation

$$(9) \qquad L_n(z) = L_n(re^{i\theta}) = \frac{1}{\pi}\int_{-\pi}^{+\pi} f(re^{i\phi})T(\theta - \phi)d\phi, \qquad (r < 1).$$

(c) In several investigations of a related kind a third method has been used, based on Fejér's result concerning the Cesàro means. Introducing in (6) for $c_\nu z^\nu$ the expression $s_\nu(z) - s_{\nu-1}(z)$ and for $s_\nu(z)$ the difference $S_\nu(z) - S_{\nu-1}(z)$ [see (7)], we obtain, for $n \geqq 2$,

$$(10) \qquad L_n(z) = \sum_{\nu=0}^{n-2} (\lambda_\nu - 2\lambda_{\nu+1} + \lambda_{\nu+2})S_\nu(z) + (\lambda_{n-1} - 2\lambda_n)S_{n-1}(z) + \lambda_n S_n(z).$$

Hence

$$(11) \qquad |L_n(z)| \leqq \sum_{\nu=0}^{n-2} |\lambda_\nu - 2\lambda_{\nu+1} + \lambda_{\nu+2}|(\nu+1) + |\lambda_{n-1} - 2\lambda_n| n + |\lambda_n|(n+1)$$

follows. This bound in general is not the exact maximum. It is attained by the function $f(z) = \epsilon = \text{const.}$, $|\epsilon| = 1$, provided the λ_ν are all real and the following inequalities hold

$$(12) \qquad \lambda_\nu - 2\lambda_{\nu+1} + \lambda_{\nu+2} \geqq 0, \qquad (\nu = 0, 1, 2, \cdots, n-2),$$
$$\lambda_{n-1} - 2\lambda_n \geqq 0, \qquad \lambda_n \geqq 0.$$

The maximum appearing on the right side is then $= \lambda_0$.*

The same method can be used to prove the non-negativeness of the trigonometric polynomial (8) if the conditions (12) are satisfied [Fejér, 11]. Thus in this case the condition mentioned in (b) is also satisfied.

* Concerning this method see in addition Fejér [10].

By means of one or the other of these methods numerous interesting results have recently been obtained for power series of class E. A short enumeration of the most typical theorems of this kind will be given now.

5. *A Theorem of Fejér and Rogosinski.* These authors have proved independently of each other [7, 24] that all partial sums of a power series of class E in $|z|<1$ are of class E in $|z|<1/2$, that is, they remain $\leqq 1$ in absolute value there. This radius $1/2$ is here the best possible; in general it cannot be replaced by a larger one.

This theorem is surprising because in the unit circle itself the partial sums of proper functions of class E become arbitrarily large (see §3).

The proof can be based, for instance, on the method (b) [Landau, 17]. Indeed, the statement is equivalent to

$$(13)\quad |c_0 + 2^{-1}c_1 z + 2^{-2}c_2 z^2 + \cdots + 2^{-n}c_n z^n| \leqq 1, \quad (|z| \leqq 1).$$

Thus we have here $\lambda_\nu = 2^{-\nu}$ and conditions (12) are satisfied because

$$\lambda_\nu - 2\lambda_{\nu+1} + \lambda_{\nu+2} = 2^{-\nu} - 2^{-\nu} + 2^{-\nu-2} = 2^{-\nu-2} > 0,$$

$$\lambda_{n-1} - 2\lambda_n = 2^{-n+1} - 2^{-n+1} = 0, \qquad \lambda_n = 2^{-n} > 0.$$

Moreover, functions of the type

$$\frac{z+\alpha}{1+\bar{\alpha}z} = \alpha + (1-|\alpha|^2)z + \cdots$$

satisfy condition E in $|z|<1$ if $|\alpha|<1$. Choosing any point t with $1/2<|t|<1$ and taking $\arg \alpha = \arg t$, we have

$$|\alpha + (1-|\alpha|^2)t| = |\alpha| + (1-|\alpha|^2)|t| > 1,$$

or $(1+|\alpha|)\,|t|>1$ provided that $|\alpha|$ is sufficiently near to 1.

6. *A Theorem of I. Schur and Szegö.* In a joint investigation with Schur [29] we noticed the fact that the preceding statement that $1/2$ is the "best" constant of the last theorem, is true only if the totality of *all* partial sums is considered. Leaving out of consideration the section $n=1$ and taking only the sections $s_n(z)$ with $n \geqq 2$, a larger circle with the same property, namely, $|z| \leqq (3/8)^{1/2} = 0.6123\ldots$, can be determined. Here the

number $(3/8)^{1/2}$ is again the best possible. This leads to the general problem of determining the greatest circle $|z| \leqq r_n$ in which all the partial sums beginning with the nth satisfy the same boundedness condition as the function. Jointly with Schur, we gave an algebraic method to calculate those numbers, and proved that $r_n \uparrow 1$. A direct computation shows

(14) $r_1=0.5, r_2=0.6123\cdots, r_3=0.6478\cdots, r_4=0.7204\cdots.$

Furthermore, we found a simple asymptotic formula for r_n if $n\to\infty$,

$$r_n = 1 - \frac{\log n - \log\log n + \log 2 + \epsilon_n}{n}, \quad (\epsilon_n \to 0). \tag{15}$$

This means that the "singular" behavior of the nth partial sum (to be >1 in absolute value) can appear only in a small strip around the unit circle whose width asymptotically $=n^{-1}\log n$ if n is large.

If the partial sums are replaced by the Cesàro means, the corresponding numbers all are $=1$ (see §3). As a generalization of the partial sums and the Cesàro means the general Cesàro means $s_n^{(k)}(z)$ can be now introduced. Thus we can determine a definite circle $|z| \leqq r_n^{(k)}$ (the greatest of this kind) in which all the Cesàro means $s_m^{(k)}(z)$, $(m \geqq n)$, of all functions $f(z)$ of class E are also of class E. Here the order k is between 0 and 1. The determination or characterization of these numbers $r_n^{(k)}$ seems to be difficult. We proved only [29, pp. 556–558] that

$$r_1^{(k)} = \frac{k+1}{2}. \tag{16}$$

7. *A Theorem of Rogosinski and Szegö.* Recalling again the fundamental property of the Cesàro means mentioned in §3, we notice that they are built up from all partial sums from the 0th to the nth. Thus the question arises to find some simple linear combinations of the n first terms expressible by some values of the nth partial sum alone, and having the same boundedness property as the Cesàro means or at any rate remaining bounded for $n\to\infty$. In a joint investigation with Rogosinski [25] we considered expressions of the form

$$As_n(ze^{a/n}) + Bs_n(ze^{b/n}), \tag{17}$$

A, B, a, b being given complex constants. The problem is to determine the values of these constants for which this expression remains bounded, uniformly for all n, for all $|z| \leqq 1$ and for all functions of class E. A necessary and sufficient condition which we obtained for this property is the equation

$$Ae^{a} + Be^{b} = 0. \tag{18}$$

The exact bound depends in general on the given constants. The proof of the boundedness can be readily given by means of method (c). The determination of the exact bound in the case (1) below has been carried out by means of (a).

This question has its origin likewise in some analogous problems concerning Fourier series.*

Two special cases should be mentioned:

(1) a and b are both pure imaginary,

(2) a and b are both real.

In case (1) our expression becomes, after multiplication by a proper constant and a proper rotation of the unit circle, .

$$e^{ia}s_n(ze^{-i\alpha/n}) - e^{-ia}s_n(ze^{i\alpha/n}), \tag{19}$$

α being a fixed real number. Here we obtained for $0 < \alpha \leqq \pi/2$, the exact bound $2\int_0^{\alpha}[J_0(x)]^2dx$, $J_0(x)$ being Bessel's function of order 0.† This statement is equivalent to the interesting inequality

$$\left|\sum_{\nu=0}^{n} \frac{\sin\left(1-\frac{\nu}{n+1}\right)\alpha}{\sin\alpha} c_\nu z^\nu\right| < |\sin\alpha|^{-1}\int_0^{\alpha}[J_0(x)]^2dx, \tag{20}$$

$$(|z| \leqq 1;\ n = 0, 1, 2, \cdots).$$

Here the right side cannot be replaced by a smaller number. For $\alpha \to 0$ we obtain again Fejér's theorem concerning Cesàro means.‡

---

* See W. Rogosinski, *Reihensummierung durch Abschnittskoppelungen*, Mathematische Zeitschrift, vol. 25 (1926), pp. 132–149.

† In a subsequent paper [36] I proved that this is true for all values of α, $\alpha > 0$.

‡ Szász had previously considered [31] this linear combination and applied method (a) without discussing the question of the maximum.

We have, for instance, for $\alpha=\pi/2$,

$$\frac{1}{2}\left| s_n(ze^{-i\pi/(2n)}) + s_n(ze^{i\pi/(2n)}) \right| < \int_0^{\pi/2} [J_0(x)]^2 dx = 1.0777\cdots. \tag{20'}$$

The last number cannot be replaced by a smaller one.

In case (2) we obtain the inequality

$$\left| s_n(\rho z) - \rho^n s_n(z) \right| \leqq 1 - \rho^n, \qquad (0 < \rho < 1), \tag{21}$$

which can be also written in the form

$$\left| \sum_{\nu=0}^{n} \frac{\rho^\nu - \rho^n}{1 - \rho^n} c_\nu z^\nu \right| \leqq 1, \quad (|z| \leqq 1; n = 0, 1, 2, \cdots). \tag{22}$$

Hence Fejér's theorem arises again as a limiting case for $\rho \to 1$. Among others we made the following curious conclusion from this inequality. Supposing $|s_n(z)| \leqq 1$ is true at a point $z=z_0$ somewhere in the unit circle for the nth section of a fixed function of our class, then the same will be true on the whole segment Oz_0, connecting z_0 with the origin. Or, the set of all points in the unit circle in which a particular section of a particular function of our class is $\leqq 1$ in absolute value defines a so-called *star-shaped* region. (Of course this always contains the origin.)

8. *Another Average of Sections.* A further remarkable property of the partial sums of the same class is that the mean value along any segment starting from the origin

$$z^{-1}\int_0^z s_n(t)dt, \qquad (|z| \leqq 1), \tag{23}$$

is $\leqq 1$ in absolute value, or it belongs to the same class as the function $f(z)$ itself [25]. This property is not at all trivial; it depends on the non-negativeness of the trigonometric polynomials

$$\frac{1}{2} + \frac{1}{2}\cos\phi + \frac{1}{3}\cos 2\phi + \cdots + \frac{1}{n+1}\cos n\phi, \tag{24}$$

the proof of which is rather troublesome [25, §5]. (The method

of Fejér [11] needs here an essential modification.) From this fact the statement follows easily by means of method (b).

9. *Harmonic Functions.* If the condition $|f(z)| \leqq 1$ is replaced by $\Re f(z) > 0$, analogous properties can be studied. If the function is normalized by the condition $\Re f(0) = 1$, the exact inequalities $|c_n| \leqq 2$, $(n = 1, 2, 3, \cdots)$, hold [Carathéodory, 1]. The analog of Landau's problem has been treated by Schur [28]. He obtained for the real part of the nth section a minimal value in $|z| \leqq 1$ which divided by n tends to min $(2 \sin x/x)$ for $n \to \infty$ (provided that the normalization $\Re f(0) = 1$ has been made). Moreover the theorem in §5 concerning the circle $|z| \leqq 1/2$ remains valid and the assertion about the numbers r_n of §6 can similarly be taken over word for word. The inequalities (21) and (23) have likewise their exact analogs for this class.

The theory of analytic functions with a positive real part is equivalent to that of positive harmonic functions. Thus the preceding results can be formulated also in terms of positive harmonic functions regular in the unit circle. If this is done the formulation of corresponding questions in space for developments in terms of *spherical harmonics* becomes possible. The analog of Schur's theorem formulated above holds for these developments [Szegö, **33**, §4] with n replaced by n^2 and the minimal value by min $(2J_1(x)/x)$, where $J_1(x)$ denotes Bessel's function of order 1. Instead of $r_1 = 1/2$ we obtain in this three-dimensional case the number $r_1 = 1/3$ [Szegö, **33**, §5], a result connected with an older remark of Pick [22],* and we can introduce the analog of the numbers r_n too. The exact determination of these new numbers r_n and the proof that they increase seems, however, to be extremely complicated. The asymptotic determination is still possible in a form somewhat different from that in the two-dimensional case. I have found recently [37]

$$r_n = 1 - \frac{2 \log n - \log \log n + \gamma + \epsilon_n}{n}, \qquad (\epsilon_n \to 0). \tag{25}$$

* Montel has recently published [Comptes Rendus, vol. 201 (1935), pp. 119–121] a note on this subject, rediscovering Pick's theorem as well as related estimates for the nth term of the development in spherical harmonics [Szegö, **33**, §3]. He does not refer to the older literature.

Here $\gamma = \log 2$ if n is odd, and $\gamma = \log(2\mu)$ if n is even, while $\mu = 0.4028\cdots$ denotes the maximum of $-J_0(x)$ for all real values of x.

10. *Polynomials.* Various extremal problems treated before can be sharpened if we consider instead of the whole class $|f(z)| \leqq 1$ or $\Re f(z) > 0$ the subset of *polynomials* of a given degree N satisfying one of these conditions in the unit circle. The same is true for developments in terms of spherical harmonics. In case of functions with a positive real part Carathéodory's inequalities (see §9) can be replaced by

$$|c_n| \leqq 2\cos\left(\frac{\pi}{\left[\frac{N}{n}\right]+2}\right), \qquad (n = 1, 2, \cdots, N;\ c_0 = 1) \tag{26}$$

[Egerváry, Lŭkács, and Szász; see Szegö, **33**, pp. 624–626]. Sidon [**30**] observed for the same class that the circle $|z| \leqq [2\cos(\pi/(N+2))]^{-1}$, instead of $|z| \leqq 1/2$, has the property mentioned in §9. Recently Levin [**18**] has obtained several results in this direction for polynomials belonging to class E. As regards three-dimensional problems of this kind see Szegö [**33**, pp. 626–632].

11. *Mean Value Conditions.* A rather obvious generalization of the boundedness property is the restriction that the integral mean value

$$\left\{\frac{1}{2\pi}\int_{-\pi}^{+\pi} |f(re^{i\phi})|^p d\phi\right\}^{1/p} \tag{27}$$

remain bounded for $r < 1$, $f(z)$ being a given function regular for $|z| < 1$. Here p denotes a fixed positive number. This condition, assuming the bound to be equal to 1, defines a class E_p. The limiting case E_∞ is the class E discussed before. The class E_2 can be characterized by the condition that the sum (2) of squares of the coefficients is convergent and $\leqq 1$. Therefore in this case it is not difficult to carry out an algebraic treatment of various questions concerning the terms, partial sums, linear combinations of terms, and so on.

More difficult is the treatment of the class E_1 corresponding to Hardy's mean value.* Numerous questions concerning coefficients, sections, and related topics can be discussed here by using the following theorem due to Fekete and M. Riesz.†

A function $f(z)$ belongs to E_1 if and only if it can be written in the form $f(z)=g(z)h(z)$, where both functions $g(z)$ and $h(z)$ belong to E_2.

This leads to the following *parametric representation* of the coefficients of $f(z)$:

$$c_n = u_0v_n + u_1v_{n-1} + \cdots + u_nv_0, \qquad (n = 0, 1, 2, \cdots).$$

$$\sum_{n=0}^{\infty} |u_n|^2 \leqq 1, \qquad \sum_{n=0}^{\infty} |v_n|^2 \leqq 1. \tag{28}$$

It is easy to show the existence of some numbers r_n depending only on n such that the partial sums of degree $\geqq n$ have a Hardy mean value $\leqq 1$ for $r \leqq r_n$ provided that the corresponding mean value of the function in the unit circle is $\leqq 1$, or else such that $s_m(z)$, $(m \geqq n)$, belong to class E_1 in $|z| \leqq r_n$ if $f(z)$ belongs to E_1 in $|z| < 1$. The number r_n should be here, of course, the largest possible. The determination of these numbers, unlike that in the limiting case E_∞, seems here to be rather difficult; their asymptotic determination may be less intricate although it has not been carried through as yet.

Using the representation (28) I have calculated the largest number r_0 for which

$$\frac{1}{2\pi}\int_{-\pi}^{+\pi} |s_1(r_0e^{i\phi})|\, d\phi \leqq 1. \tag{29}$$

The result is $r_0 = (2\mu^{1/2})^{-1} = 0.9146\cdots$, where μ is the maximum of the function

---

* G. H. Hardy, *The mean value of the modulus of an analytic function*, Proceedings of the London Mathematical Society (2), vol. 14 (1915), pp. 269–277.

† Verbal communication. The proof can be based on the following facts: (i) Any function $f(z)$ of class E_1 regular in $|z| \leqq 1$ can be written in the form $f(z)=l(z)q(z)$, $l(z)$ being a rational function regular and with $|l(z)|<1$ in $|z|<1$, $q(z)$ a regular function of class E_1 and $\neq 0$ in $|z|<1$. (ii) From any set of functions $\{f_\nu(z)\}$ belonging to E_2 a subset can be selected which is uniformly convergent in any circle $|z| \leqq r$, $(r<1)$. Another direct (but less elementary) way would be to make use of the factorization theorem of F. Riesz, Mathematische Zeitschrift, vol. 18 (1923), pp. 87–95.

$$(30) \qquad x^{-2}\left(\pi^{-1}\int_0^{\pi}(1+x^2-2x\cos\phi)^{1/2}\,d\phi-1\right)$$

for $x>1$, or the maximum of

$$(31) \qquad (\sin\alpha/2)^2(\cos\alpha/2)^{-4}(E(\sin\alpha)-(\sin\alpha/2)^2)$$

for $0<\alpha<\pi/2$, and $E(k)$ denotes Legendre's elliptic integral of the second kind

$$(32) \qquad E(k)=\frac{2}{\pi}\int_0^{\pi/2}(1-k^2\sin^2\phi)^{1/2}\,d\phi.$$

These results show that all these questions have a more complicated character than in the case E_∞.

12. *Univalent Bounded Functions.* A very interesting subset of $E=E_\infty$ can be obtained by imposing upon $f(z)$ the additional condition to be univalent or simple in the unit circle $|z|<1$. Fejér [8, see also 9] proved that the partial sums of a power series of this kind remain *uniformly bounded* in $|z|<1$. He obtained by application of his Cesàro mean theorem the bound $1.7071\cdots$. Using (20′) I found [35, §3] a better estimate $1.6160\cdots$. Recently Levin [18, §4] succeeded in improving this result; the exact bound, however, is not known as yet.

In all these investigations the univalency of the function is used only to a very moderate extent, namely, in the following form: The area of the w-set in the conformal representation $w=f(z)$ corresponding to $|z|<1$ is $\leqq\pi$, whence

$$(33) \qquad |c_1|^2+2|c_2|^2+3|c_3|^2+\cdots+n|c_n|^2+\cdots\leqq 1.$$

The results mentioned remain valid for the larger subset of E satisfying this condition. Levin investigated [18, §3] some generalizations of this class requiring, besides E, the inequality

$$(34) \qquad \alpha_1|c_1|^2+\alpha_2|c_2|^2+\cdots+\alpha_n|c_n|^2+\cdots\leqq 1,$$

where $\{\alpha_n\}$ is a given sequence of positive numbers.

13. *Univalent Functions.* Another rather complicated class is that of the univalent functions (without the condition E). The best known general limitation for the coefficients has been obtained by Littlewood [19, pp. 498–499]. It is: $|c_n|<en$ provided that $c_1=1$. The analog of the numbers r_n can be defined

here as well, requiring univalency of $s_m(z)$, $(m \geqq n)$, for $|z| < r_n$, but nothing is known about their determination and properties in general, doubtless a rather intricate question. I proved [35] that $r_1 = 1/4$, or each section remains univalent in the circle $|z| < 1/4$, a number which cannot be replaced by a larger one. An asymptotic characterization of the r_n for $n \to \infty$ seems also to present some difficulties; however, these might not be insurmountable.

The methods used in the treatment of these problems are not quite simple. In general, Koebe's distortion theorem* is needed, sometimes even Löwner's theory of univalent functions.†

14. *Related Classes.* Even more difficult is the treatment of "odd" univalent functions, that is, univalent functions of the form (1) with $c_2 = c_4 = c_6 = \cdots = 0$. Littlewood and Paley proved [20] that in this case $|c_n| < K$, $c_1 = 1$, K being an absolute constant.

The treatment of star-shaped and convex representations is possible by using more elementary methods, primarily Carathéodory's theory of functions with a positive real part.

Various elegant results have been recently found for univalent power series of the form (1) with *real* coefficients. For instance, the exact inequality $|c_n| \leqq n$, $(n = 2, 3, 4, \cdots)$, holds in this case, $c_1 = 1$ [Dieudonné, 4; Rogosinski, 26]. More generally, Rogosinski [26] studied power series of the form (1) assuming real values if and only if z itself is real. He obtains a complete characterization of this class (called "typisch-reell") in terms of the coefficients.

Fejér examined [12, pp. 61–62] univalent functions with real coefficients having the property that the image of the unit circle has at most two points of intersections with every straight line parallel to the imaginary axis. The partial sums are in this case univalent in $|z| < 1/4$‡ and even in $|z| < 3^{-1/2}$ if all the $c_{2\nu}$ disappear.

By generalizing and combining these classes, numerous vari-

* See, for instance, G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, (1925), vol. 2, p. 27, problem 151.

† K. Löwner, *Untersuchungen über schlichte konforme Abbildungen des Einheitskreises*, Mathematische Annalen, vol. 89 (1923), pp. 103–121.

‡ Which is generally true for univalent functions (see above), but it can be proved much more easily in this case.

ations of the problem regarding the partial sums are possible [see, for instance, Takahashi, **38** and Noshiro, **21**].

15. *Power Series with Monotonic Coefficients.* Finally another point of view likewise appearing in various recent investigations may be mentioned in a few words. Introduction of proper regularity properties for the whole sequence of coefficients is possible. We can expect then an analogous regular behaviour of the partial sums, of the remainder sums, of some linear combination of the terms, and so on. From this point of view Fejér has recently investigated [**13, 15**] trigonometric and power series, the coefficients of which are monotonic of a definite order k, that is, having positive 0th, 1st, 2nd, $\cdots$, kth differences. In this case certain positiveness, monotone character, or convexity properties of the partial sums can be proved. Furthermore, in a joint paper with Fejér [**14**] we introduced the notion of monotonic convergence of a complex sequence $\{s_n\}$ to the limit s requiring the monotonic convergence of the positive numbers $|s_n - s|$ to 0. We showed that this property holds for the partial sums of any power series, provided that the coefficients are monotonic of the order 2. However, it does not hold generally for power series with only simply monotonic coefficients. More exactly we have proved

$$(35) \qquad |f(z)| \geqq |f(z) - s_0(z)| \geqq \cdots \geqq |f(z) - s_n(z)| \geqq \cdots .$$

As a consequence of this fact we obtain

$$(36) \qquad |f(z) - s_n(z)| \leqq |f(z)| \quad \text{and hence} \quad |s_n(x)| \leqq 2|f(z)|.$$

A simple special case is that of the binomial series $f(z) = (1-z)^{-\rho}$ if $0 < \rho < 1$. The second inequality (36) corresponding to this case has been previously obtained, with a positive constant A instead of 2, by Chapman [**3**] and M. Riesz [**23**]; it has importance for the summability theory of Fourier and Laplace series. As regards a direct proof see Szegö [**32**].

Assuming the so-called total monotony of the coefficients, the behaviour of the partial sums becomes still more regular. See Fejér [**13**].

Some of these results can be extended to integrals of the form

$$\int_0^{+\infty} f(t)e^{-zt}dt$$

which have properties analogous to those of power series.

16. *Conclusion.* Numerous variations and analogs of the preceding problems are possible and some of them can be solved in a more or less exhaustive way. It would be a long task to give a complete account of this topic. Our intention was to set forth only the most typical results of this field, illustrating the way in which properties of an analytic function are reflected in the terms or in the sections of its power series development. A great many open problems in this direction can be formulated easily. Only a general analytic taste is able to decide which of these questions is worth being dealt with and to what extent they are connected with characteristic properties of analytic functions.

Bibliography

1. C. Carathéodory, *Über den Variabilitätsbereich der Fourierschen Konstanten von positiven harmonischen Funktionen*, Rendiconti del Circolo matematico di Palermo, vol. 32 (1911), pp. 193–217.

2. C. Carathéodory and L. Fejér, *Über den Zusammenhang der Extremen von harmonischen Funktionen mit ihren Koeffizienten und über den Picard-Landauschen Satz*, Rendiconti del Circolo matematico di Palermo, vol. 32 (1911), pp. 218–239.

3. S. Chapman, *On non-integral orders of summability of series and integrals*, Proceedings of the London Mathematical Society, (2), vol. 9 (1910), pp. 369–409.

4. J. Dieudonné, *Recherches sur quelques problèmes relatifs aux polynomes et aux fonctions bornées d'une variable complexe*, Annales Scientifiques École Normale Supérieure, (3), vol. 48 (1931), pp. 247–358.

5. L. Fejér, *Über gewisse Potenzreihen an der Konvergenzgrenze*, Sitzungsberichte der math.-phys. Klasse der Bayerischen Akademie, 1910, Nr. 3, pp. 1–17.

6. L. Fejér, *Über gewisse durch die Fourier'sche und Laplace'sche Reihe definierte Mittelkurven und Mittelflächen*, Rendiconti del Circolo matematico di Palermo, vol. 38 (1914), pp. 79–97.

7. L. Fejér, *Über die Positivität von Summen, die nach trigonometrischen oder Legendre'schen Funktionen fortschreiten.* (Erste Mitteilung.) Acta litterarum ac scientiarum Reg. Universitatis Hungaricae, sectio scient.-math., vol. 2 (1925), pp. 75–86.

8. L. Fejér, *Über die Koeffizientensumme einer beschränkten und schlichten Potenzreihe*, Acta Mathematica, vol. 49 (1926), pp. 183–190.

9. L. Fejér, *Über die Grenzen der Abschnitte gewisser Potenzreihen*, Acta litterarum ac scientiarum Reg. Universitatis Hungaricae, sectio scient.-math., vol. 4 (1928), pp. 14–24.

10. L. Fejér, *Einige Sätze, die sich auf das Vorzeichen einer ganzen rationalen Funktion beziehen; nebst Anwendungen dieser Sätze auf die Abschnitte und Abschnittsmittelwerte von ebenen und räumlichen harmonischen Entwicklungen und von beschränkten Potenzreihen*, Monatshefte für Mathematik und Physik, vol. 35 (1928), pp. 305–344.

11. L. Fejér, *Über ein trigonometrisches Analogon eines Kakeyaschen Satzes*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 38 (1929), pp. 231–238.

12. L. Fejér, *Neue Eigenschaften der Mittelwerte bei den Fourierreihen*, Journal of the London Mathematical Society, vol. 8 (1933), pp. 53–62.

13. L. Fejér, *Potenzreihen mit mehrfach monotoner Koeffizientenfolge und ihre Legendrepolynome*, Proceedings of the Cambridge Philosophical Society, vol. 31 (1935), pp. 307–316.

14. L. Fejér and G. Szegö, *Über die monotone Konvergenz von Potenzreihen mit mehrfach monotoner Koeffizientenfolge*, Prace Matematyczno-Fizyczne, vol. 44 (1935), pp. 1–11.

15. L. Fejér, *Trigonometrische Reihen und Potenzreihen mit mehrfach monotoner Koeffizientenfolge*, Transactions of this Society, vol. 39 (1936), pp. 18–59.

16. E. Landau, *Abschätzung der Koeffizientensumme einer Potenzreihe*, Archiv der Mathematik und Physik, (3), vol. 21 (1913), pp. 42–50 and pp. 250–255; vol. 24 (1916), pp. 250–260.

17. E. Landau, *Über einen Fejérschen Satz*, Nachrichten der Gesellschaft der Wissenschaften zu Göttingen, math.-phys. Klasse, 1925, p. 22.

18. V. Levin, *Über die Koeffizientensummen einiger Klassen von Potenzreihen*, Mathematische Zeitschrift, vol. 38 (1934), pp. 565–590.

19. J. E. Littlewood, *On inequalities in the theory of functions*, Proceedings of the London Mathematical Society, (2), vol. 23 (1924), pp. 481–519.

20. J. E. Littlewood and R. E. A. C. Paley, *A proof that an odd schlicht function has bounded coefficients*, Journal of the London Mathematical Society, vol. 7 (1932), pp. 167–169.

21. K. Noshiro, *On the theory of schlicht functions*, Journal of the Faculty of Science, Japanese Imperial University, (1), vol. 2 (1934), pp. 129–155.

22. G. Pick, *Ein Abschätzungssatz für positive Newtonsche Potentiale*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 23 (1915), pp. 329–332.

23. M. Riesz, *Sur la sommation des séries de Fourier*, Acta litterarum ac scientiarum Reg. Universitatis Hungaricae, sectio scient.-math., vol. 1 (1923), pp. 104–113.

24. W. Rogosinski, *Über Bildschranken bei Potenzreihen und ihren Abschnitten*, Mathematische Zeitschrift, vol. 17 (1923), pp. 260–276.

25. W. Rogosinski and G. Szegö, *Über die Abschnitte von Potenzreihen, die in einem Kreise beschränkt bleiben*, Mathematische Zeitschrift, vol. 28 (1928), pp. 73–94.

26. W. Rogosinski, *Über positive harmonische Entwicklungen und typisch-reelle Potenzreihen*, Mathematische Zeitschrift, vol. 35 (1932), pp. 93–121.

27. I. Schur, *Über Potenzreihen, die im Innern des Einheitskreises beschränkt sind*, Journal für Mathematik, vol. 147 (1917), pp. 205–232; vol. 148 (1918), pp. 122–145.

28. I. Schur, *Über die Koeffizientensummen einer Potenzreihe mit positivem reellen Teil*, Archiv der Mathematik und Physik, (3), vol. 27 (1918), pp. 126–135.

29. I. Schur and G. Szegö, *Über die Abschnitte einer im Einheitskreise beschränkten Potenzreihe*, Sitzungsberichte der preussischen Akademie, 1925, pp. 545–560.

30. S. Sidon, *Ein Satz über positive harmonische Polynome*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 35 (1926), pp. 97–99.

31. O. Szász, *Ungleichungen für die Koeffizienten einer Potenzreihe*, Mathematische Zeitschrift, vol. 1 (1918), pp. 163–183.

32. G. Szegö, *Bemerkungen zu einer Arbeit von Herrn Fejér über die Legendreschen Polynome*, Mathematische Zeitschrift, vol. 25 (1926), pp. 172–187.

33. G. Szegö, *Koeffizientenabschätzungen bei ebenen und räumlichen harmonischen Entwicklungen*, Mathematische Annalen, vol. 96 (1927), pp. 601–632.

34. G. Szegö, *Korlátos hatványsorokra vonatkozó újabb vizsgálatokról*, Matematikai és Physikai Lapok, vol. 35 (1928), pp. 70–95.

35. G. Szegö, *Zur Theorie der schlichten Abbildungen*, Mathematische Annalen, vol. 100 (1928), pp. 188–211.

36. G. Szegö, *Zur Theorie der Legendreschen Polynome*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 40 (1931), pp. 163–166.

37. G. Szegö, *Über räumliche harmonische Entwicklungen, welche in der Einheitskugel positiv sind*, Monatshefte für Mathematik und Physik, vol. 43 (1936), pp. 148–156.

38. S. Takahashi, *Über die Abschnitte einer ungeraden schlichten Potenzreihen*, Proceedings of the Physico-Mathematical Society of Japan, (3), vol. 16 (1934), pp. 7–15.

39. O. Toeplitz, *Über die Fouriersche Entwicklung positiver Funktionen*, Rendiconti del Circolo matematico di Palermo, vol. 32 (1911), pp. 191–192.

WASHINGTON UNIVERSITY,
ST. LOUIS

A NOTE ON THE ASSOCIATIVE LAW IN LOGICAL ALGEBRAS*

BY H. B. CURRY

1. *Introduction.* In 1925 Bernays published† a proof that within the formalism of the *Principia Mathematica* the proposition "Assoc" could be derived from the other primitive propositions. The purpose of this note is to give an alternative proof which brings out the fact that a similar conclusion holds in a variety of other systems, described hereunder as systems B.‡ The proof is essentially a refinement of that given by Schröder in his *Vorlesungen über die Algebra der Logik*, vol. 1, pp. 255–257, and credited to C. S. Peirce.§

2. *Definition of Systems A and B.* A system A is a system consisting of a class K containing a rule of combination (which we may call multiplication and denote by simple juxtaposition), and a relation $<$ such that‖

I. $p<pp$.

II. $pq<q$.

III. $pq<qp$.

IV. *If* $p<q$ *and* $q<r$, *then* $p<r$.

A system B is a system A which has the additional properties:

V. *If* $p<q$, *then* $rp<rq$.

VI. *If* $p<q$ *and* $p<r$, *then* $p<qr$.

THEOREM 1. *If a system A has either of the properties* V, VI, *it has the other, and so is a system B.*

---

* Presented to the Society, January 2, 1936.

† Mathematische Zeitschrift, vol. 25, p. 312.

‡ Bernays' proof is also valid in a system B. Indeed, he recognizes (footnote 6, loc. cit.) that his proof is valid in more general systems, although he does not formulate any explicit limitations on them.

§ Thus the present proof contains nothing essentially new and is probably known to several writers. The author has been led to publish it solely by the fact that the validity of Peirce's proof under these circumstances appears not to be universally realized; certainly it was overlooked by the authors of the *Principia*.

‖ It should be recognized that I–VI are non-formal statements about the system concerned and not mere formulas. It is, of course, a weaker hypothesis that such rules hold than that formulas to the same effect are provable.

PROOF. (1) Suppose V holds. Then if $p<r$, we have $qp<qr$ by V, and $pq<qp$ by III, hence $pq<qr$ by IV. If $p<q$, then $pp<pq$ by V, $p<pp$ by I, hence $p<pq$ by IV. From these two conclusions we have $p<qr$ by IV, so that VI holds.

(2) Suppose VI holds. Then, if $p<q$, $rp<q$ by II, IV, and $rp<r$ by III, II, IV; hence $rp<rq$ by VI, and so V holds.

THEOREM 2. *In any system B, if* $p<q_1, p<q_2, \cdots, p<q_n$, *and if r is any combination of* $q_1, q_2, \cdots, q_n$, *then* $p<r$.

PROOF. The combination r is constructed out of the q_i by performing a number of times the operation of finding the product of two factors. At each stage of this process if the relation holds between p and both of the factors, it holds between p and the product by VI; since it holds between p and all the q_i it holds, by induction, between p and r.

The property proved in Theorem 2 contains all forms of the associative law as special cases. For if p is any combination which involves q_i, then $p<q_i$ by repeated applications of II, III, IV; as, for example, $q_2(q_1q_3)<q_1q_3<q_3q_1<q_1$. Hence we have the following theorem.

THEOREM 3. *In any system B the associative laws*

$$p(qr) < (pq)r, \qquad (pq)r < p(qr), \qquad p(qr) < q(pr)$$

all hold.

3. *Application to the Principia Mathematica.* Here interpret pq as $p \vee q$, $p<q$ as $\vdash .q \supset p$. Then I, II, III are *Taut*, *Add*, and *Perm*, respectively, while IV and V both follow from *Sum* and the rule of inference. Hence I-V all hold and the system is a system B by Theorem 1.

4. *On the Converse of Theorem* 3. That the associative laws may hold in a system A in which V does not hold is shown by Bernays' second independence example.* For here we may let pq be interpreted as $p \vee q$ and let $p<q$ hold when and only when $\sim q \vee p=\alpha$. Then I-IV and the associative laws hold, while V fails for $p=\beta$, $q=\delta$, $r=\gamma$.

THE PENNSYLVANIA STATE COLLEGE

* Loc. cit., Gruppe II on p. 318.

A GENERALIZATION OF WARING'S PROBLEM*

BY L. E. DICKSON

1. *Introduction.* Define $g(n, m)$ so that every integer $\geqq m$ is a sum of g nth powers, while not every integer $\geqq m$ is a sum of $g-1$ powers. It is customary to write $g(n)$ for $g(n, 0)=g(n, 1)$. Quite recently I evaluated $g(n)$ for every $n>6$.

For $n=9$ or 11, I evaluate $g(n, m)$ for each m below specified large values M. In particular, $g(11, M)=336$ and $g(9, M)=163$ are small compared with $g(11)=2132$ and $g(9)=548$.

By use of the Hardy-Littlewood Theory and extensive tables, it was found that $g(6)\leqq 160$. I here obtain $g(6)\leqq 110$.

2. *Asymptotic Theory.* Recently I proved† that, if $n\geqq 4$, every integer $\geqq N$ is a sum of $s-2+3k$ integral nth powers $\geqq 0$, where the quantities are defined as follows. Let p^θ be the highest power of the prime p which divides n. Write $\gamma=\theta+1$ if $p>2$, $\gamma=\theta+2$ if $p=2$. Let D be the g.c.d. of $p-1$ and n/p^θ. Write $m=D(p^\gamma-1)/(p-1)$. Then the conditions on s (for Lemma B of A) are $s>2n$, $s\geqq m+1$, for every prime p. They hold for $s\geqq 13$ if $n=6$, and for $s\geqq 2n+1$ if n is an odd prime or its square.

Employ natural logarithms. If $\vartheta(b)$ is the sum of the logarithms of all primes $\leqq b$,

$$\vartheta(b) \leqq \frac{6}{5}(.92129)b + 3\log^2 b + 8\log b + 5.$$

Take

$$b = (1+n^s)^{2/(s-5)},$$

$$-\log c = \log n + (n+1)\log 3 + 2n^2\log 2 + n(2n-1)\vartheta(b),$$

$$C = 12(8n\cdot 3^{n-1})^{1/2}2^{(n-1)/4}n^{3(n-1)/2}/(3/2)^{(1-1/n)/2},$$

$$N^{-J/n} = C/c, \quad 2J = \sigma\left(3-\frac{1}{2n}\right)+z-\frac{(n-1)}{2n^2},$$

* Presented to the Society, October 26, 1935.

† Annals of Mathematics, vol. 37 (1936), pp. 293–316, cited as A; American Journal of Mathematics, July, 1936, cited as J.

$$\sigma = n\left(1 - \frac{1}{n}\right)^k, \qquad k > \log r/\{\log n - \log (n-1)\},$$
$$r = n^2(6n-1)/(n-1-2n^2z),$$

where z is positive and so small that

$$1 + \log (3/2)^{n-1} + (n-1)/(2n^2)\cdot\log N \leqq \left(\frac{1}{3} N^{1/n}\right)^z.$$

3. *Case* $n=6$. The best result is obtained from $s=19$. Take $z=0.00002$. Then the least integer k is 31. Using base 10 except as marked, we get

$$\log \sigma = \bar{2}.3235310, \qquad -J = 0.0039946, \qquad \vartheta(b) = 257.984,$$
$$-\log_e c = 17086.33198, \qquad \log_e C = 2.11363,$$
$$\log\log N = 7.047165.$$

All integers $<l=2120044$ are sums of 86 sixth powers,* while all between l and $L_0=51\ 679\ 845\ 000\ 000$ are sums of 33 sixth powers. Then† all integers between l and L_t are sums of $t+33$ if $\log\log L_t = (0.0791813)t + 0.9563804$. Thus $L_t \geqq N$ if $t=77$. But $t+33=110=s-2+3k$.

THEOREM 1. *Every positive integer is a sum of* 110 *sixth powers.*

4. *Case* $n=11$. Take $z=0.00001$. The least integer k is 70. Also $s \geqq 23$. The best result is obtained from $k=100$, $s=43$. Then

$$\log \sigma = \bar{4}.90212, \qquad -J = 0.0194770, \qquad \vartheta(b) = 388.19352,$$
$$-\log_e c = 89856.02131, \quad \log_e C < \frac{1}{2} n^2, \quad \log\log N = 7.343518.$$

Denote the eleventh powers of $2, \cdots, 9$ by $a, \cdots, h$. By an extended algebraic table (in MS), I proved that every integer between

$$l = 2g + h = 48\ 560\ 928\ 793$$

and $l+15b$ is a sum of 129 eleventh powers. By ascents, all between l and $L_0 = 33\ 348\ 227 \times 10^6$ are sums of 171, and all between l and L_t are sums of $t+171$, where

---

* R. C. Shook, University of Chicago Dissertation, 1934.

† This Bulletin, vol. 39 (1933), p. 711, Theorem 12. Here $\nu = 1/6$ to seven decimal places.

$$\log\log L_t = t\log 1.1 + 0.3140358.$$

Hence $L_t \geqq N$ if $t \geqq 170$.

LEMMA 1. *Every integer* $\geqq l$ *is a sum of* 341 *eleventh powers.*

Elsewhere* I proved that 302 eleventh powers suffice from $j = 2d+e = 460\ 453\ 306$ to $j+14c$ and are necessary for $j+66a+8b+9c+1416$, while by ascent 321 powers suffice from j to far beyond l.

LEMMA 2. *Every integer* $\geqq j$ *is a sum of* 341 *eleventh powers.*

5. To obtain further results for $n = 11$, employ

(1) $b = 86a + 1019, \qquad c = 23b + 38a + 1139,$

(2) $d = 11c + 15b + 16a + 808, \qquad e = 7d + 5c + 14a - 11.$

My method† to construct an algebraic table of minimum decompositions is based on leaders L. Since L has a decomposition into fewer powers, the same is true of the sum of L and any linear function. The leaders $< e$ are

$$173a(=10+2b),\ 64a+165b,\ 36a+189b,\ 356b,\ 253b+c,$$
$$75a+38b+10c,\ 86a+27c,\ 164b+28c,\ 24a+140b+29c,$$
$$35a+13b+46c,\ 115b+65c,\ 82c,\ 126a+d,\ 127b+d,$$
$$115a+63b+2d,\ 87a+87b+2d,\ 40a+25b+3d.$$

Employ linear homogeneous functions in which the coefficients of a, b, c, d are $\geqq -86$, -23, -11, -7, respectively, by (1) and (2), and which have no leader as component. We obtain $87a-b=1029$, 25 equations in a, b, c, 33 with $-d$, 25 with $-2d$, 17 with $-3d$, 14 with $-4d$, 12 with $-5d$, 10 with $-6d$, and 8 with $-7d$.

We shall say that there is a *peak* (x, m), or peak x at m, if m is a sum of x, but not fewer, nth powers, while all integers $> m$ are sums of fewer than x powers. Thus m is the greatest integer requiring x nth powers. If (x', m') and (x, m) are consecutive peaks, every integer between m' and m is a sum of x nth powers.

THEOREM 2. *There are exactly* 24 *peaks* $\geqq 336$ *if* $n = 11$. *They include*

* Journal of the London Mathematical Society, vol. 9 (1934), pp. 201–206.

† This Bulletin, vol. 40 (1934), pp. 487–493. More details in American Mathematical Monthly, vol. 41 (1934), pp. 547–555.

$P_j = (1185-119(j-1),\ jc+85a+2047-120j)$, $(j=1, 2, 3)$;
$R_k = (838-119k,\ (4+k)c+85a+1577-120k)$, $(k=0, 1, 2, 3)$;
$S = (954,\ 3c+82a+1697)$.

If (x, m) *is any of these peaks except* R_3, *also* $(x-93,\ m+22b)$ *is a peak. Together, these give the peaks with* $x = 1185, 1092, 1066, 973, 954, 947, 861, 854, 838, 745, 719, 626, 600, 507, 481$. *The earlier peaks are* $(2132,\ u=85a+2047)$, $(1211,\ u+22\text{b})$. *The later peaks are*

$(454,\ d+4c+9b+5a+529)$, $(383,\ 2d+2c+16b+24a+1769)$, $(373,\ w+47a+769)$, $(372,\ w+75a+740)$, $(357,\ w+83a+740)$, $(354,\ 3d+2c+17b+36a+762)$, $(336,\ 6d+2c+17b+36a+743)$,

where $w = 2d+2c+17b$.

6. *Case* $n=9$. Take $z=0.00001$. The least integer k is 54. Also $s \geqq 19$. We take $s=30$, $k=80$, and obtain

$$\log \sigma = \bar{4}.8620425, \quad -J = 0.0236148, \quad \vartheta(b) = 346.26604,$$

$$-\log_e c = 53104.1773, \quad \log_e C < \frac{1}{2}n^2, \quad \log\log N = 6.9443023.$$

If $a, \cdots, e$ denote the ninth powers of $2, \cdots, 6$, I proved* that all integers between $h=2d+e$ and $L_0 = 58221534000$ are sums of 140 ninth powers. By ascent as in §3, all between h and L_t are sums of $t+140$ if

$$\log\log L_t = (0.0511525)t + 0.3376543.$$

Then $L_t \geqq N$ if $t=130$. This proves the following lemma.

LEMMA 3. *Every integer* $\geqq h=2d+e$ *is a sum of* 270 *ninth powers.*

THEOREM 3. *There are exactly* 19 *peaks* $\geqq 163$ *if* $n=9$. *If* (x, m) *is one of the four peaks* $(314,\ c+25a+390)$, $(220,\ c+12b+25a+284)$, $(207,\ 3c+12b+25a+269)$, $(194,\ 5c+12b+25a+254)$, *then* $(x-5,\ m+12a)$ *is a peak. The further peaks are* $(548,\ 37a+511)$, $(333,\ 12b+37a+284)$, $(208,\ 2c+37a+390)$, $(195,\ 4c+37a+375)$, $(182,\ 6c+37a+360)$, $(181,\ d+6b+25a+220)$, $(177,\ d+7b+12a+492)$, $(176,\ d+7b+26a+477)$, $(175,\ d+8b+2a+235)$, $(169,\ d+8b+11a+220)$, $(163,\ 2d+11b+12a+473)$.

* This Bulletin, vol. 40 (1934), pp. 487–493.

The first four peaks give the greatest integers requiring 548, 333, 314, 309 ninth powers, respectively. There is very strong evidence that a like result holds for the next 15 peaks. For example, all integers between $e+d$ and $e+2d$ are sums of 128 ninth powers; all between $e+2d$ and $e+3d$ are sums of 125.

UNIVERSITY OF CHICAGO

MAPS OF ABSTRACT TOPOLOGICAL SPACES IN BANACH SPACES*

BY A. D. MICHAL AND E. W. PAXSON

1. *Introduction.* This paper is to serve as a brief introduction to the method of considering the analysis of abstract topological spaces through the medium of homeomorphic mappings of these spaces on subsets of Banach spaces.† Our primary objective here, however, is to obtain for some general topological groups the abstract correspondents of the fundamental Lie partial differential equations for an r-parameter continuous group.‡ The essential notion is the treatment of the general situation with the aid of abstract *coordinates* in Banach spaces wherein the Fréchet differential may be used.§

By an abstract topological space is meant here a set of elements of completely unspecified nature, together with an undefined concept, that of neighborhood of an element (we denote the elements by small Latin letters, and the neighborhood associated with an element a by $U(a)$), satisfying the four Hausdorff postulates given below.‖

---

* Presented to the Society, November 30, 1935.

† S. Banach, *Théorie des Opérations Linéaires*, 1932.

‡ S. Lie, *Theorie der Transformationsgruppen*, vols. 1, 3.

§ M. Fréchet, *Annales de l'École Normale Supérieure*, (3), vol. 42 (1925), p. 293. Briefly, $f(x)$ on B_1 to B_2 has a differential at $x=x_0$, if there exists a function $f(x;\ z)$ on B_1^2 to B_2, linear (additive and continuous) in z and such that given a $\rho>0$ there is determined a $n>0$, so that $\|f(x_0+z)-f(x_0)-f(x_0;\ z)\| \leqq \rho\|z\|$ for $\|z\| \leqq n(\rho)$; $f(x_0;\ z)$ is the differential. See also various papers by Hildebrandt, Graves, Kerner, Michal, and many others.

‖ F. Hausdorff, *Mengenlehre*, 1927, pp. 226–229.

(1) $a \epsilon U(a)$.

(2) $b \epsilon U(a) . \supset : \exists U(b) . U(b) \subset U(a)$.

(3) $U_1(a) \cap U_2(a) \supset U_3(a)$.

(4) $a \neq b . \supset : . \exists U(a) . U(b) : U(a) \cap U(b) = (0)$.

A Banach space is a linear, normed abstract space with real multipliers. If the multipliers are complex, one speaks of a complex Banach space. The fundamental notions of point-set theory and the logical calculus of classes is assumed. By a homeomorphic mapping we mean the customary bi-unique, bi-continuous correspondence of one set of elements to another.*

2. *Types of Mapping.* The first type of mapping between the two spaces is effected as follows. Let Σ be an open subset in the Banach space B. Map homeomorphically every neighborhood in the topological space T on this same set Σ. Note that such a mapping implies the postulation of an infinite character for the space T, since, using postulate (2) above, one has $U(a) h \Sigma$, and $U(b) h \Sigma$ with $U(b) \subset U(a)$. But since homeomorphism is transitive, $U(a) h U(b)$. Then $U(a)$ has the same potency as one of its proper subsets, so that, in the Dedekind sense, it is infinite.

Now consider the intersection C of two neighborhoods $U(\bar{a})$, $U(\bar{b})$, $C = U(\bar{a}) \cap U(\bar{b})$. Then by the mappings† $\alpha = f_{\bar{a}}(c)$, $\beta = f_{\bar{b}}(c)$ one has $\alpha = f_{\bar{a}}(f_{\bar{b}}^{-1}(\beta)) = \phi(\beta)$. Thus $\phi(\beta)$ is a homeomorphic map of Σ^1 on Σ^2, since its composing functions are homeomorphisms. Hence we have the following theorem.

THEOREM 1. *The intersection of two neighborhoods in T determines a homeomorphic mapping of one subset Σ^1 of Σ on to another, Σ^2.*

We now make the following definitions:

DEFINITION 1. The value α of $f_{\bar{a}}(a)$ will be called the abstract coordinate of a in the Banach space B.

DEFINITION 2. The class of homeomorphic transformations $\{\alpha = \phi(\beta)\}$ will be called the class of abstract coordinate transformations for the class $\{C\}$.

---

* W. Sierpinski, *General Topology*, 1934. When two sets E_1, E_2 are homeomorphic under a mapping function f, one writes $E_1 h_f E_2$.

† If $x \epsilon U(\bar{x})$, we write $\alpha = f_{\bar{x}}(x)$, $x = f_{\bar{x}}^{-1}(\alpha)$; $x \epsilon T$, $\alpha \epsilon \Sigma$.

All possible intersections of neighborhoods in T determine, by Theorem 1, homeomorphic mappings of various parts of Σ on various other parts.

DEFINITION 3. If all such point transformations possess Fréchet differentials up to and including the rth ($r \geqq 1$), the complete mapping will be called r-differentiable.

THEOREM 2. *For a complex Banach space a* 1*-differentiable map is analytic.*

PROOF. By known theorems,* the existence of a first Fréchet differential implies that the function is continuous, that it possesses a Gateaux differential, and hence that the function, and so the map, is analytic.

THEOREM 3. *Let* $c = t(d)$ *map homeomorphically* C^1 *on* C^2, *where* C^1, $C^2 \subset C$. *Then there are induced two distinct homeomorphic maps of two distinct subsets of* Σ *on two other distinct subsets.*

PROOF. $\alpha = f_a(c)$, $\beta = f_b(c)$; $\gamma = f_a(d)$, $\delta = f_b(d)$. Then $\alpha = f_a(t(f_a^{-1}(\gamma))) = \theta_a(\gamma)$ homeomorphically, and $\beta = f_b(t(f_b^{-1}(\delta))) = \theta_b(\delta)$ homeomorphically, where $\alpha, \beta, \gamma, \delta$ are typical elements in distinct subsets of Σ.

THEOREM 4. *Every homeomorphic point transformation on* Σ^1 *to* Σ^2 (Σ^1, $\Sigma^2 \subset \Sigma$) *is an abstract coordinate transformation.*

PROOF. Let the transformation be $\delta = \psi(\mu)$. Then there exists a neighborhood $U(\bar{x})$ such that for $z \epsilon U(\bar{x})$, $\mu = f_x(z)$. Hence $\delta = \psi(f_{\bar{x}}(z))$, or there exists a mapping function distinct from $f_{\bar{x}}$, so that $\delta = f_{\bar{y}}(z)$. This implies that there exists a $U(\bar{y}) h_{f_{\bar{y}}} \Sigma$, where $z \epsilon U(\bar{x}) \cap U(\bar{y})$. Hence $\delta = \psi(\mu)$ is a true coordinate transformation.

For an r-differentiable map, considering Theorems 3 and 4, one may make the following definitions.

DEFINITION 4. A homeomorphic point transformation $c = t(d)$ on C^1 to C^2 in the intersection C will be said to be of class $C^{(r)}$.

DEFINITION 5. For a complex Banach space and a 1-differentiable map, $c = t(d)$ will be called an analytic transformation. (See Theorem 2.)

---

* A. E. Taylor, California Institute of Technology thesis, (1936); see also this Bulletin, vol. 41 (1935), p. 800, abstract 41-11-424, and Graves, this Bulletin, vol. 41 (1935), pp. 641-662.

As an example of these definitions take the conformal mapping of one complex plane (T) on another (B). The interiors of circles about points are taken as neighborhoods in T, each one going over into the same suitably chosen open set in B. Then as is readily seen, for analytic mapping, $c=t(d)$ is analytic, in the ordinary sense.

THEOREM 5. *Every $c=t(d)$ (as in Definition 4) determines four points, distinct from c and d, each one of which is in a neighborhood intersection in T.*

PROOF. $\alpha=f_a(c)$, $\beta=f_b(c)$; $\gamma=f_a(d)$, $\delta=f_b(d)$. Hence $\alpha=f_a(t(f_a^{-1}(\gamma)))=\theta_a(\gamma)$ and $\beta=\theta_b(\delta)$. Also, by the transitivity of homeomorphism $\alpha=\phi_a(\delta)$, $\beta=\phi_b(\gamma)$. By Theorem 4, these represent coordinate transformations for four distinct points in T.

DEFINITION 6. A regular abstract coordinate transformation of class r is an abstract coordinate transformation possessing differentials up to and including the rth, where the rth differential is continuous.

3. *Group Function.* Now we let the topological space T support a group under the composition function $c=g(a, b)$. Further let this group be right-continuous. That is, if a be fixed, and c', b' are variables so that $c'=g(a, b')$, the existence of a $U(c)$ implies the existence of a $U(b)$ such that $U(c) \supset g(a, U(b))$. Hence, as is known, $g(a, U(b))$ is a neighborhood of c, say $U(c)$. Now take any three elements of T, a, b, c and two fixed elements f, h. Then the functions $c'=g(f, b')$, $b'=g(h, a')$ may be considered. One has $c'=g(f, g(h, a'))=g(g(f, h), a')=g(k, a')$.

If a' ranges over at least part of some $U(\bar{a})$, it follows that there will be a $U(\bar{b})$ over part of which b' will range, and a $U(\bar{c})$ over part of which c' will range, by continuity. Then there exist mapping functions $f_{\bar{a}}$, $f_{\bar{b}}$, $f_{\bar{c}}$ such that $\alpha'=f_{\bar{a}}(a')$, $\beta'=f_{\bar{b}}(b')$, $\gamma'=f_{\bar{c}}(c')$, wherein α', β', γ' range over at least parts of Σ. The group function g defines a homeomorphism of c to b in $c=g(a, b)$. Then

$$c' = g(f, b'):\gamma' = f_{\bar{c}}(g(f, f_{\bar{b}}^{-1}(\beta'))) = \mu(\beta'),$$

$$b' = g(h, a'):\beta' = f_{\bar{b}}(g(h, f_{\bar{a}}^{-1}(\alpha'))) = \nu(\alpha'),$$

$$c' = g(k, a'):\gamma' = f_{\bar{c}}(g(k, f_{\bar{a}}^{-1}(\alpha'))) = \rho(\alpha').$$

where $\gamma' h_\mu \beta'$, $\beta' h_\nu \alpha'$, and hence $\gamma' h_{\mu\nu} \alpha'$, that is, $\gamma' = \mu(\nu(\alpha'))$ $= \rho(\alpha')$. But by Theorem 4, there are determined e_1', e_2', e_3'; $e_1' \epsilon U_1 \cdot \overline{U}_1, \cdots$, where the e's are not, in general, in any of the neighborhoods above, and for which μ, ν, ρ are coordinate transformations

$$\gamma' = f_1(e_1'), \quad \beta' = \bar{f}_1(e_1'), \cdots$$

Consequently, if the whole mapping is r-differentiable, one has

$$\text{(A)} \qquad \rho(\alpha'; \delta\alpha') = \mu(\nu(\alpha'); \nu(\alpha'; \delta\alpha')).$$

Write

$$\text{(A')} \qquad \begin{aligned} \rho(\alpha'; \delta\alpha') &= R(\gamma', \alpha', \delta\alpha'), \\ \gamma' &= f_{\bar{c}}(c'), \quad \alpha' = f_{\bar{a}}(a'). \end{aligned}$$

Consider a neighborhood $U(\bar{c}_1)$ that intersects $U(\bar{c})$, and a $U(\bar{a}_1)$ that intersects $U(\bar{a})$. Then there are determined for certain subsets of values of c', a' coordinate transformations. In fact

$$\gamma' = f_{\bar{c}}(c'), \quad \gamma_1' = f_{\bar{c}_1}(c'), \qquad (\gamma_1' \neq \gamma'),$$

for values of c' satisfying both of these. Similarly

$$\alpha' = f_{\bar{a}}(a'), \quad \alpha_1' = f_{\bar{a}_1}(a'), \qquad (\alpha_1' \neq \alpha').$$

Then

$$\gamma_1' = f_{\bar{c}_1}(f_{\bar{c}}^{-1}(\gamma')) = \theta(\gamma')$$

and

$$\alpha_1' = f_{\bar{a}_1}(f_{\bar{a}}^{-1}(\alpha')) = \tau(\alpha')$$

are the coordinate transformations. Note that the ranges of possible values for γ' and α' are not as extensive as before.

But between any γ_1' and any α_1' there exists a coordinate transformation determining a point p in the intersection of two $U(\bar{x})$, $U(\bar{y})$, with $\gamma_1' = f_{\bar{x}}(p')$, $\alpha_1' = f_{\bar{y}}(p')$, $\gamma_1' = f_{\bar{x}}(f_{\bar{y}}^{-1}(\alpha_1')) = \phi(\alpha_1')$, wherein ϕ has a first Fréchet differential. The coordinate transformation mentioned above is necessarily the same for the whole set γ_1' into the whole set α_1'. For, writing $\phi(\alpha_1')$ explicitly, we have

$$\gamma' = f_{\bar{c}}(g(k, f_{\bar{c}}^{-1}(\alpha'))) = \rho(\alpha') \text{ so that } \gamma_1' = \theta(\rho(\tau^{-1}(\alpha_1'))),$$

that is,

$$\gamma_1' = f_{\bar{c}_1}(f_{\bar{c}}^{-1}(f_{\bar{c}}(g(k, f_{\bar{a}}^{-1}(f_{\bar{a}}(f_{\bar{a}_1}^{-1}(\alpha_1')))))))),$$
$$\gamma_1' = f_{\bar{c}_1}(g(k, f_{\bar{a}_1}^{-1}(\alpha_1'))) = \rho_1(\alpha') = \phi(\alpha_1').$$

(Note the formal invariance of the ρ function.) Hence we have

(B) $$\rho_1(\alpha_1'; \delta\alpha_1') = \theta(\rho(\tau^{-1}(\alpha_1')); \rho(\tau^{-1}(\alpha_1'); \tau^{-1}(\alpha_1'; \delta\alpha_1'))).$$

Now (A) may be written

(C) $$R_1(\gamma_1', \alpha_1', \delta\alpha_1') = \theta(\gamma'; R(\gamma', \alpha', \delta\alpha')),$$

since $\tau^{-1}(\alpha_1'; \delta\alpha_1') = \delta\alpha'$, where $\gamma_1' = \theta(\gamma')$.

Equation (C) indicates that $R(\gamma', \alpha', \delta\alpha')$ transforms like an abstract contravariant tensor of rank 1, with respect to γ'. With respect to α' and $\delta\alpha'$ the function is scalar.

If in (A′) one puts $\alpha' = \gamma'$,

$$\rho(\alpha'; \delta\alpha') = R(\alpha', \alpha', \delta\alpha') = \delta\alpha'.$$

Further, from (A) and (A′),

$$R(\gamma', \alpha', \delta\alpha') = R(\gamma', \beta', R(\beta', \alpha', \delta\alpha')).$$

Hence, if $\gamma' = \alpha'$, $R(\gamma', \beta', \delta\beta')$ is inverse to $R(\beta', \gamma', \delta\beta')$. So $R(\gamma', \beta', \delta\alpha')$ is a solvable linear function of $\delta\alpha'$ with inverse $R(\beta', \gamma', \delta\alpha')$. R vanishes if and only if $\delta\alpha' = 0$. We remark that for an r-differentiable map the quantities R possess continuous Fréchet differentials up to the $(r-2)$th order.

Now $\mu(\beta'; \delta\beta') = R(\gamma', \alpha', R(\alpha', \beta', \delta\beta'))$, where $\gamma' = \mu(\beta')$, so that μ is independent of α'. Then we may put $\alpha' = \alpha_0$, where α_0 is the correspondent in Σ of the identity element a_0 of the topological group. Define

$$R(\gamma', \alpha_0, \delta\beta') .= . R'(\gamma', \delta\beta'),$$
$$R(\alpha_0, \gamma', \delta\beta') .= . R(\gamma', \delta\beta'),$$

where the R and R' on the right are inverse. *Then the fundamental differential equation of Lie type, satisfied representatively in the Banach space by the continuous topological group function, is*

(D) $$\mu(\beta'; \delta\beta') = R'(\mu(\beta'), R(\beta', \delta\beta')).$$

California Institute of Technology

INVOLUTORIAL SPACE TRANSFORMATIONS ASSOCIATED WITH A RATIONAL RULED SURFACE*

BY L. A. DYE

1. *Introduction.* The present paper concerns various new types of Cremona involutorial transformations in S_3. Each one is a sample of an infinite category, and the concept can be extended to higher spaces.

Transformations obtained by joining corresponding points of curves or by associating the points of a curve with a projective pencil of surfaces have been studied from time to time and are sketched in the *Encyklopädie*, the *Repertorium*, and particularly in *Selected Topics of Algebraic Geometry*, including the Supplementary Report (Bulletin 63, National Research Council, 1928, No. 96, 1934). All these papers can be found in *Topics*, Chapters 8, 9, or Supplement, Chapters 4, 5 under the names Black, Carroll, Davis, DePaoli, Dye, Moffa, Montesano, Sharpe, and Snyder.

The types here discussed can not be put into any of the categories previously mentioned. The complex of lines defined by pairs PP' of associated points is not linear, is not special, and does not have any particular role in the problem. In most of the earlier cases it was formed by the secants to a given curve, or was linear. In the DePaoli types the lines PP' describe a congruence, each line containing an infinite number of pairs of conjugate points.

The procedure used in this paper is to establish a (1, 1) correspondence between the generators of a ruled surface R and the surfaces of a pencil $|F|$. A general point P of space selects a surface F of the pencil and hence the associated generator r of R. The plane π determined by r and P is tangent to R at a point Q. The line PQ meets the surface F in P and a residual point P'; any other intersections are accounted for by properly relating $|F|$ and R. The points P, P' are an associated pair in an involutorial transformation under which the pencil $|F|$ and the congruence of conics cut from $|F|$ by the planes π are invariant.

* Presented to the Society, February 23, 1935, and November 30, 1935.

2. *Pencil of Quadrics through a C_4, $(p=1)$.* A pencil of quadric surfaces $|F_2|:C_4$ having an elliptic quartic curve in common, and a ruled surface $R_{n+1}:l^n$ of order $n+1$ with an n-fold line l determine an involutorial transformation of order $8n+5$. In this transformation there are two fundamental curves of the first species; one is the C_4 which is the base of $|F_2|$ and the other is a C_{2n+3} which is the locus of the piercing points of the lines r and their associated quadrics. The image of each of these points is a conic and the conics generate the image surface L_{8n+4} of C_{2n+3}.

There are $2n-2$ torsal generators on R_{n+1}. The tangent planes along them cut conics from the associated quadrics which are parasitic, since every point of such a generator may be taken as a point Q in the tangent plane, and hence the image of every point of the conic is the whole conic.

Through each generator r there are two planes which cut degenerate conics from the associated quadric. If the point of contact Q of such a plane is on one of the lines of the degenerate conic, then every point of the line will go into the whole line, and the line is parasitic. The number of such lines is $8n+8$ and is determined by taking the complete intersection of two homoloidal surfaces.

In any plane π the points of contact of the tangents drawn from Q to the conic section lie on the invariant surface K_{4n+4} of the transformation. When Q is a point of C_{2n+3}, then that point will lie on both K and L, and these surfaces will have contact along C_{2n+3}.

Let the equation of R_{n+1} be $ax_2+bx_3+cx_4=0$, where a, b, c are binary forms of order n in x_1, x_2. The equations of the line l are $x_1=x_2=0$, and any plane through l such as $\mu x_1-\lambda x_2=0$ cuts from R_{n+1} a line r whose equations may be written as follows: $\mu x_1-\lambda x_2=\bar{a}x_2+\bar{b}x_3+\bar{c}x_4=0$, where $\bar{a}=a(\lambda, \mu), \cdots$. The plane π determined by a point $P(y)$ and the line r is tangent to R_{n+1} at the point $Q(z)$ which has the coordinates $(\lambda A_0R, \mu A_0R, \mu B_0R-n\bar{c}M, \mu C_0R+n\bar{b}M)$, where $A_0\equiv\bar{b}_1\bar{c}_2-\bar{b}_2\bar{c}_1, \cdots$, and $\bar{a}_i\equiv\partial a/\partial x_i|_{\lambda,\mu}, \cdots$. The symbols R, M represent the forms $\mu y_1-\lambda y_2$, $\bar{a}y_2+\bar{b}y_3+\bar{c}y_4$, respectively.

Let the equation of the pencil of quadrics be $\mu F_2'-\lambda F_2''=0$. A point $P(y)$ determines a quadric F_2 which the line PQ meets in the residual point $P'(y')$, where $y_i'=y_iL-z_iK$, and $L\equiv F_2(z)$,

$K \equiv y_i \partial F(z)/\partial z_i$. The equations of the transformation are obtained by replacing λ, μ by $F_2'(y), F_2''(y)$ in y_i'.

The table of characteristics of the transformation is

$$S_1 \sim S_{8n+5} : C_4^{4n+1} + C_{2n+3}^{2+2t},$$
$$C_{2n+3} \sim L_{8n+4} : C_4^{4n+1} + C_{2n+3}^{2+t},$$
$$C_4 \sim F_{16n+8} : C_4^{8n+1} + C_{2n+3}^{4+4t},$$
$$K_{4n+4} : C_4^{2n+1} + C_{2n+3}^{1+t}.$$

The superscript t is used to indicate that the multiplicity is due to contact; for example, the tangent planes to the two sheets of an S_{8n+5} through C_{2n+3} coincide at each point of C_{2n+3} with the tangent plane to K_{4n+4} at the point. The nature of the surface F_{16n+8} is obtained by finding the transform of a quadric F_2.

3. *Pencil of Quadrics through the Line l.* If the basis curve of the pencil of quadrics consists of the line l and a residual space cubic, then the equation of $|F_2|$ may be written in the form $|F_2| = x_1(\alpha x) + x_2(\beta x) = 0$, where (αx) is a linear homogeneous form in x_i and $\alpha_i \equiv \mu\alpha_i' - \lambda\alpha_i'', \cdots$. The form $F_2(z)$ is composite and has the factors $A_0 R[\lambda(\alpha z) + \mu(\beta z)] \equiv A_0 RL$. The equations of the transformation are $y_i' = y_i A_0 RL - z_i K$, but $y_i' = A_0 R^2[(\beta z) - \lambda A_0\{\lambda(\alpha y) + \mu(\beta y)\}]$, and $y_2' = A_0 R^2[(\beta z) + \mu A_0\{\lambda(\alpha y) + \mu(\beta y)\}]$.

When a plane π passes through l, the point of contact $Q(z)$ is at the intersection of l and r. Such a plane cuts from F_2 a line meeting l elsewhere than at Q. The image of the line is Q, and as Q moves on l, the image lines generate the surface $R_3 = 0$ taken twice. At any point on l the tangent planes to the $2n$ sheets of a homoloidal surface coincide in pairs with the n tangent planes to $M_{2n+1} = 0$ at that point, since the highest powers of y_3, y_4 have $(\bar{b}y_3 + \bar{c}y_4)^2$ as a factor in the equation of an S_{8n+5}, and $(\bar{b}y_3 + \bar{c}y_4)$ in the case of L_{4n+5}. The invariant surface K_{4n+4} does not have contact along l, but in the intersection of K_{4n+4}, and on S_{8n+5} the line l must be counted an additional n times.

In this transformation each generator r meets its associated quadric in a point on l, and one residual point. The locus of these residual points is a fundamental curve C_{n+3}, $(p = 0)$, which has the surface L_{4n+5} as its image.

The $2n-2$ pinch points of R_{n+1} along l are fundamental points of the transformation, since each of these points is associated with all the planes through its torsal generator. The image of a pinch point is the quadric surface associated with the torsal generator through the point. The equations of these quadrics are obtained by putting A_0 equal to zero.

The number of parasitic lines due to the point $Q(z)$ lying on a degenerate conic cut from F_2 by a plane π is $4n+5$, and the number of parasitic conics is $2n-2$ as before. The table of characteristics of the transformation is

$$
\begin{aligned}
S_1 &\sim S_{8n+5} : l^{4n+2} + n\bar{l}^2 + C_3^{4n+1} + C_{n+3}^{2+2l} + (2n-2)O_i^{4n+5}, \\
l &\sim 2R_3 \quad : l^2 \qquad\quad + C_3 \quad + C_{n+3} + (2n-2)O_i^2, \\
C_{n+3} &\sim L_{4n+5} : l^{2n+2} + n\bar{l} \quad + C_3^{2n+2} + C_{n+3}^{1+l} + (2n-2)O_i^{2n+3}, \\
C_3 &\sim F_{12n+6} : l^{6n+1} + n\bar{l}^4 + C_3^{6n+2} + C_{n+3}^{2+2l} + (2n-2)O_i^{6n+5}, \\
(2n-2)O_i &\sim A_{4n-4} : l^{2n-2} \qquad + C_3^{2n-2} \qquad + (2n-2)O_i^{2n-1}, \\
K_{4n+4} &: l^{2n+2} \qquad + C_3^{2n+1} + C_3^{1+l} + (2n-2)O_i^{2n+3},
\end{aligned}
$$

where the notation $\bar{l}$ is used to indicate contact along l.

4. *Pencil of Cubic Surfaces with a Double Line.* A pencil of cubic surfaces $|F_3|$ having a double line l and a rational twisted quintic C_5 as a base is made projective with the pencil of planes $|p|$ through l. A general point P will determine a surface F_3 and the plane p which corresponds to F_3. The plane p will cut from F_3 a line r which generates a ruled quartic surface $R_4 : l^3$. The pencil $|F_3|$ and the surface R_4 determine a transformation in the manner described in the introduction.

Let the equation of the pencil of cubic surfaces be $ax_2+bx_3+cx_4=0$, where a, b, c are binary quadratic forms in x_1, x_2, and $a_{ij} \equiv \mu a_{ij}' - \lambda a_{ij}''$, $\cdots$. The equations of the planes p and of the line r have the same form as those used in §2. The ruled quartic R_4 has the equation $x_2F_3' - x_1F_3'' = 0$. The plane π determined by a point $P(y)$ and the line r is tangent to R_4 at the point $Q(z)$, where

$$(z_i) \equiv (\lambda AR,\ \mu AR,\ \mu BR - 2\bar{c}M,\ \mu CR + 2\bar{b}M),$$

in which $A \equiv A_0 + 2A^0$, $\cdots$, and $A^0 \equiv \bar{b}'\bar{c}'' - \bar{b}''\bar{c}'$, $\cdots$.

The residual intersection of the line PQ with the associated surface F_3 is the point $P'(y')$, where

$$y_i' = y_i\left(z_i\frac{\partial F(y)}{\partial y_i}\right) z_i\left(y_i\frac{\partial F(z)}{\partial z_i}\right).$$

Replacing λ, μ by $F'(y)$, $F''(y)$, we have $y_i' = R^3(y_iAL - z_iK)$. The forms L, K can be expressed as follows:

$$\begin{aligned} L &\equiv a_1A^0 + b_1B^0 + c_1C^0 - A^0N, \\ N &\equiv 2\mu y_2\alpha - (\mu y_1 + \lambda y_2)\beta + 2\lambda y_1\gamma, \\ K &\equiv N[2\lambda y_1A_{22} - (\mu y_1 + \lambda y_2)A_{12} + 2\mu y_2A_{11}] \\ &\quad + 2\mu RD - A(\alpha y_2^2 - \beta y_1y_2 + \gamma y_1^2). \end{aligned}$$

The letters α, β, γ represent the second-order determinants of the matrix

$$\left\| \begin{matrix} a_{11}'y_2+b_{11}'y_3+c_{11}'y_4 & a_{12}'y_2+b_{12}'y_3+c_{12}'y_4 & a_{22}'y_2+b_{22}'y_3+c_{22}'y_4 \\ a_{11}''y_2+b_{11}''y_3+c_{11}''y_4 & a_{12}''y_2+b_{12}''y_3+c_{12}''y_4 & a_{22}''y_2+b_{22}''y_3+c_{22}''y_4 \end{matrix} \right\|,$$

and A_{ij} are the cofactors of a_{ij} in $D \equiv |a_{11}b_{12}c_{22}|$.

When a point Q is at the intersection of r and C_5, the plane π is tangent to both R_4 and F_3, since the line r and the tangent to C_5 determine the plane π. The image of each point of C_5, when it plays this role, is the residual conic cut from F_3 by π. These conics generate the surface L_{18}. The C_5 has another image surface, however, since it also enters the transformation as a part of the base of $|F_3|$. This other image surface is obtained by transforming an F_3 and is of order 48. Geometrically this surface is generated by the images of the four points of C_5 not on r in any plane π.

In this transformation each line r is a parasitic line and the surface R_4 generated by these lines factors out of the transformation three times. The line l is a multiple parasitic line along which S_{31} and L_{18} have contact, since the highest powers of y_3, y_4 in their equations have N_6 as a factor.

The surfaces L_{18} and K_{16} have contact along C_5 as in the other transformations. The four pinch points O_i of R_4 along l are fundamental, and the tangent planes along the four torsal generators cut conics from the associated F_3's which are parasitic in the transformation. The number of parasitic lines is 14 as determined by the complete intersection of two S_{31}'s. The table of characteristics of the transformation is

$$
\begin{aligned}
S_1 &\sim S_{31}: l^{19} + 3\bar{l} + C_5^{10+2t} + 4O_i^{22},\\
C_5 &\sim L_{18}: l^{11} + 3\bar{l} + C_5^{6+t} + 4O_i^{12},\\
F_{48} &: l^{28} + 3\bar{l}^2 + C_5^{15+5t} + 4O_i^{34},\\
4O_i &\sim A_{12}: l^{8} + C_5^{4} + 4O_i^{9},\\
K_{16} &: l^{10} + C_5^{5+t} + 4O_i^{11}.
\end{aligned}
$$

5. *Pencil of Cubic Surfaces with Two Double Points.* The transformation to be developed here is similar to the one in the preceding section. A pencil of cubic surfaces $|F_3|$ through two double points O_i contains the line through them and has a residual basis curve C_8 of order 8 with triple points at O_i. Each F_3 is tangent to a fixed plane along the line l through O_i. These tangent planes cut lines r from their associated F_3 and the lines r generate a ruled quartic surface $R_4: l^2$.

Let $ax_2+bx_3+cx_4+(\mu x_1-\lambda x_2)x_3x_4=0$ be the equation of the $|F_3|$. The equations of the lines r and the surface R_4 and the coordinates of the points $Q(z)$ are the same as those in the last section.

When λ, μ are replaced by $F_3'(y)$, $F_3''(y)$, the form M is factorable into R and another factor, which is of the sixth order in y and contains a term $(y_3y_4)^2$. The factor R^2 comes off from the equations of the transformation and we have $y_i' = y_iL - z_iK$.

The curve C_8 meets each generator r in two points at which R_4 and the associated F_3 have contact. The image of C_8 consists of two surfaces; one is the L_{30} due to the contact of $|F_3|$ with R_4 along C_8, and the other surface is an F_{60} due to the C_8 being a part of the base of $|F_3|$.

The lines r are all parasitic and the line l is a multiple parasitic line. There are 24 parasitic lines which are not generators of R_4, and 4 parasitic conics. The surfaces L_{30} and S_{31} have contact along l, and the surfaces K_{16} and L_{30} have contact along C_8. The table of characteristics of the transformation is

$$
\begin{aligned}
S_1 &\sim S_{31}: l^{6} + 6\bar{l} + C_8^{10+2t},\\
C_8 &\sim L_{30}: l^{6} + 6\bar{l} + C_8^{10+t},\\
F_{60} &: l^{11} + 6\bar{l}^2 + C_8^{19+5t},\\
K_{16} &: l^{4} + C_8^{5+t}.
\end{aligned}
$$

THE CITADEL, CHARLESTON, S. C.

ON RATIONAL AUTOMORPHS OF BINARY QUADRATIC FORMS*

BY GORDON PALL

1. *Introduction.* We consider in this paper those rational automorphs which carry an integral solution (x, y) of

$$ax^2 + bxy + cy^2 = n \tag{1}$$

into an integral solution. Further properties are treated in §§6, 7.

By classical methods for finding all algebraic automorphs, and expressing the conditions for the coefficients to be rational, we have the following known result.

THEOREM 1. *The general proper rational automorph (of determinant 1) of a primitive form $f = [a, b, c]$ of non-zero discriminant $d = b^2 - 4ac$ is*

$$A = \begin{pmatrix} (t - bu)/2 & -cu \\ au & (t + bu)/2 \end{pmatrix}, \tag{2}$$

and the general improper rational automorph (of determinant -1) is

$$B = \begin{pmatrix} (t - bu)/2 & (b/a)(t - bu)/2 + cu \\ au & -(t - bu)/2 \end{pmatrix}, \tag{3}$$

where t, u range over all rational solutions of

$$t^2 - du^2 = 4. \tag{4}$$

The reciprocal automorph is obtained from (2) by changing u to $-u$, from (3) by changing the signs of both t and u; thus $B^{-1} = -B$.

2. *Denominator of a Rational Automorph.* The *denominator* of a rational automorph is the least common denominator of its four coefficients. To obtain all automorphs (2) having denominator m we write $t = T/m$, $u = U/m$, where T, U, m are any integers satisfying

$$T^2 - dU^2 = 4m^2, \qquad \text{g.c.d. } (m, U) = 1. \tag{5}$$

* Presented to the Society, October 26, 1935.

For any common divisor of m, aU, $(T+bU)/2$, $(T-bU)/2$, cU is a divisor of aU, bU, cU, and hence is 1, f being primitive.

Let Δ denote the denominator of (3) with the substitution $t=T/m$, $u=U/m$ satisfying (5). Evidently $\Delta \mid am$. Further $aU/m=k/\Delta$, $U/m=k/(a\Delta)$, where U/m is in lowest terms. Hence $m \mid a\Delta$.

3. *Transform of an Automorph.* If A is a rational automorph of f, and S is a unitary integral transformation carrying f into $f'=[a', b', c']$, then $A' \equiv S^{-1}AS$ is a rational automorph of f' having the same denominator as A. For multiplication by integral matrices cannot increase the denominator, and we can solve for $A=SA'S^{-1}$.

Let ξ_i denote the matrix of one column consisting of two elements x_i, y_i. Let the integral solution ξ_1 of (1) be carried into the integral solution $\xi_2=A^{-1}\xi_1$, by the rational automorph A. Then the automorph $S^{-1}AS$ of f' carries the integral solution $S^{-1}\xi_1$ of

$$a'x^2 + b'xy + c'y^2 = n \tag{6}$$

into the integral solution $S^{-1}\xi_2$ of (6).

4. THEOREM 2. *The denominator of any rational automorph of $[a, b, c]$ which carries an integral solution of* (1) *into an integral solution must be a divisor of n.*

As regards (2), we merely multiply by $-y$ and x and combine

$$\frac{1}{2}(T - bU)x - cUy \equiv 0, \quad aUx + \frac{1}{2}(T + bU)y \equiv 0 \pmod{m},$$

to obtain $U(ax^2+bxy+cy^2) \equiv 0$, whence $n \equiv 0 \pmod{m}$.

For (3) we have similarly $aUx-(T-bU)y/2 \equiv 0 \pmod{m}$,

$$\frac{1}{2}(T - bU)ax + \left\{\frac{1}{2}(T - bU)b + acU\right\}y \equiv 0 \pmod{am},$$

whence $(T+bU)ax/2+acUy \equiv 0 \pmod{m}$, $aU(ax^2+bxy+cy^2) \equiv 0$, and finally $an \equiv 0 \pmod{m}$. Thus $\Delta \mid a^2n$. Employing as in §3 an equivalent form with a' prime to a, $\Delta \mid a'^2n$. Hence $\Delta \mid n$.

5. THEOREM 3. *Any two integral solutions of* (1) *can be transformed into each other by proper (and improper) rational automorphs of $[a, b, c]$.*

For from $ax_i^2+bx_iy_i+cy_i^2=n$, $(i=1, 2)$, follows

$$T^2 - dU^2 = 4n^2, \quad T = 2ax_1x_2 + b(x_1y_2 + x_2y_1) + 2cy_1y_2, \quad U = x_1y_2 - x_2y_1. \tag{7}$$

Let A denote (2) with $(t, u)=(T/n, -U/n)$. We find that $A^{-1}\xi_1=\xi_2$. If B denotes (3) for this (t, u), $B\xi_1=(x_2+by_2/a, -y_2)$.

Let $\delta=$g.c.d.(x_2, y_2). Let the unitary transformation

$$S = \begin{pmatrix} x_2/\delta & h \\ y_2/\delta & k \end{pmatrix}, \qquad (kx_2 - hy_2 = \delta),$$

carry f into f', where $a'=n/\delta^2$. Evidently $S^{-1}\xi_2$ is the solution $x=\delta$, $y=0$ of (6). Define T', U' by (7) with f' for f, $S^{-1}\xi_1$ and $S^{-1}\xi_2$ for ξ_1 and ξ_2, and let B' denote the corresponding automorph (3) of f' with $t=-T'/n$, $u=U'/n$. Then B' carries $S^{-1}\xi_1$ into $S^{-1}\xi_2$, and the automorph $SB'S^{-1}$ of f carries ξ_1 into ξ_2.

6. *Product of Rational Automorphs.* Let A_i and B_i denote (2) and (3), respectively, with $(t, u)=(T_i/m_i, U_i/m_i)$; and let $m_3=m_1m_2$, $T_i^2-dU_i^2=4m_i^2$, $(i=1, 2, 3)$. Then $A_1A_2=A_3$ and $A_1B_2=B_3$, where

$$2T_3 = T_1T_2 + dU_1U_2, \qquad 2U_3 = T_1U_2 + T_2U_1. \tag{8}$$

Also $B_1B_2=A_3$ and $B_1A_2=B_3$, where in place of (8) we have

$$2T_3 = T_1T_2 - dU_1U_2, \qquad 2U_3 = U_1T_2 - U_2T_1. \tag{9}$$

COROLLARIES. $A_1A_2=A_2A_1$, $B_1B_2=(B_2B_1)^{-1}$, $A_1B_2=A_2B_1=B_1A_2^{-1}=B_2A_1^{-1}$.

7. *Rational Automorphs of Denominator mn.* It is not in general true, even if m and n are relative-prime, that a rational automorph of denominator mn can be expressed as a product of rational automorphs of denominators m and n. This is true of a wide variety of classes even with $h(d)>1$; for example, of $[2, 1, 3]$ of discriminant $d=-23$. But for the principal form $[1, 1, 6]$ of this discriminant there are rational automorphs of denominator 6, but none (proper or improper) of denominators 2 and 3.

The parametric solution of (5) may be useful; for each factorization $d=rs$, we have $m=(ru_1^2-su_2^2)/4$, $u=u_1u_2$, $t=(ru_1^2+su_2^2)/2$, where u_1 and u_2 are integers of g.c.d. 1 or 2, and m is an integer prime to u.

Two rational automorphs A_1 and A_2 of f may be called *right-equivalent* if there exists an integral automorph I of f such that $A_1 I = A_2$. If (T_1, U_1) and (T_2, U_2) belong to the same set* of solutions of (5), the corresponding automorphs (with $t = T_i/m$, $u = U_i/m$) are readily seen to be right-equivalent.

McGILL UNIVERSITY

A NOTE ON RECURSIVE FUNCTIONS†

BY S. C. KLEENE

The notion of a recursive function of natural numbers, which is familiar in the special cases associated with primitive recursions, Ackermann-Péter multiple recursions, and others, has received a general formulation from Herbrand and Gödel. The resulting notion is of especial interest, since the intuitive notion of a "constructive" or "effectively calculable" function of natural numbers can be identified with it very satisfactorily.‡ Consider the operation of passing from a function $\rho(x_1, \cdots, x_n, y)$, such that for each set of values of $x_1, \cdots, x_n$ the equation $\rho(x_1, \cdots, x_n, y) = 0$ has solutions for y, to the function "$\epsilon y[\rho(x_1, \cdots, x_n, y) = 0]$" of which the least solution is $x_1, \cdots, x_n$. We have shown that the (general) recursive functions are the functions which are derivable from the primitive recursive functions by one application of this operation and of substitution.§ Herein we note the related result, that the recursive functions are the functions obtainable by repeated applications of the operation just described and of substitution from the three particular functions $x+y$ (sum), $x \cdot y$ (product), δ_y^z (Kronecker delta). This result follows from the other by an adaptation of an argument used by Gödel in proof that every

---

* For definition of set, see Pall, Transactions of this Society, vol. 35 (1933), p. 491; or Dirichlet, *Vorlesungen über Zahlentheorie*, §87.

† Presented to the Society, January 1, 1936.

‡ See A. Church, *An unsolvable problem of elementary number theory*, American Journal of Mathematics, vol. 58 (1936), pp. 345–363, §7.

§ S. C. Kleene, *General recursive functions of natural numbers*, Mathematische Annalen, vol. 112 (1936), No. 5, IV and V.

primitive recursive relation is arithmetic, which we now present.* In doing so, we duplicate in part the analysis of primitive recursive functions given by Hilbert and Bernays.† For the notation and terminology, see our cited article.

DEFINITION 1. Let C denote the least class of functions such that $x+y$, $x \cdot y$, δ_y^x, $U_i^n(x_1, \cdots, x_n) \epsilon C$, if $\theta(y_1, \cdots, y_m)$, $\chi_1(\mathfrak{x}), \cdots, \chi_m(\mathfrak{x}) \epsilon C$, then $\theta(\chi_1(\mathfrak{x}), \cdots, \chi_m(\mathfrak{x})) \epsilon C$, and if $\rho(\mathfrak{x}, y) \epsilon C$ and $(\mathfrak{x})(Ey)[\rho(\mathfrak{x}, y)=0]$, then $\epsilon y[\rho(\mathfrak{x}, y)=0] \epsilon C$.

Instead of the identity functions $U_i^n(x_1, \cdots, x_n)=x_i$, a second substitution schema $\theta(\chi_1(\mathfrak{x}), \chi_2(\mathfrak{y}))$ may be introduced.

Using the identity functions, we can replace substitutions which do not fall under the given schema by series of substitutions which do thus, $\theta(x, \phi(x, y, z), \psi(z, y))=\theta(U_1^3(x, y, z), \phi(x, y, z), \psi(U_3^3(x, y, z), U_2^3(x, y, z)))$.

DEFINITION 2. A relation ϵC if its representing function ϵC.

Analogously to Gödel's I–IV:

I. The functions $C(x)$, $S(x)$, $U_i^n(x_1, \cdots, x_n) \epsilon C$. Every function (relation) obtained by substitution of functions which ϵC for variables of functions (relations) which $\epsilon C \epsilon C$. If the relation $R(\mathfrak{x}, y) \epsilon C$ and $(\mathfrak{x})(Ey)R(\mathfrak{x}, y)$, then $\epsilon y[R(\mathfrak{x}, y)] \epsilon C$.

II. If the relations R, $S \epsilon C$, so do $\overline{R}$, $R \vee S$ (hence also $R \& S$).

III. If the functions $\phi(\mathfrak{x})$, $\psi(\mathfrak{y}) \epsilon C$, so does the relation $\phi(\mathfrak{x})=\psi(\mathfrak{y})$.

IV. If the function $\phi(\mathfrak{x})$ and the relation $R(x, \mathfrak{y}) \epsilon C$, so do the relations $(x)[x<\phi(\mathfrak{x}) \rightarrow R(x, \mathfrak{y})]$ and $(Ex)[x<\phi(\mathfrak{x}) \& R(x, \mathfrak{y})]$.

Proofs. $C(x)=\epsilon y[x \cdot y=0]$. Let $\alpha(x)=\epsilon y[\delta_y^x=0]$. Then $\alpha(0)=1$, $\alpha(1)=0$. $S(x)=x+\alpha(C(x))$. For II we see that, if $\rho(\mathfrak{x})$ and $\sigma(\mathfrak{y})$ are the representing functions of R and S, $\alpha(\rho(\mathfrak{x}))$ is the representing function of $\overline{R}$ and $\rho(\mathfrak{x}) \cdot \sigma(\mathfrak{y})$ is the representing function of $R \vee S$. Let $\gamma(x, y)=\alpha(\delta_y^x)$. Then $\gamma(x, x)=0$ and $\gamma(x, y)=1$ for $x \neq y$. III holds since $\gamma(\phi(\mathfrak{x}), \psi(\mathfrak{y}))$ is the representing function of $\phi(\mathfrak{x})=\psi(\mathfrak{y})$. In proof of IV, we have

$$(x)[x<\phi(\mathfrak{x}) \rightarrow R(x, \mathfrak{y})] \equiv \epsilon x[\overline{R(x, \mathfrak{y}) \vee x=\phi(\mathfrak{x})}]=\phi(\mathfrak{x}),$$

$$(Ex)[x<\phi(\mathfrak{x}) \& R(x, \mathfrak{y})] \equiv \overline{(x)[x<\phi(\mathfrak{x}) \rightarrow \overline{R(x, \mathfrak{y})}]}.$$

V. $x<y \epsilon C$. $x \equiv y \pmod{n} \epsilon C$.

---

* Kurt Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik, vol. 38 (1931), pp. 173–198, Satz VII.

† Hilbert-Bernays, *Grundlagen der Mathematik*, vol. 1, pp. 412–421.

For

$$x<y \equiv \overline{(Ez)}[z<x+1 \& x=y+z],\ [x \equiv y (\mathrm{mod}\ n)]$$
$$\equiv (Ez)[z<x+y+1 \& \{x=y+z\cdot n \vee y=x+z\cdot n\}],$$

(see Gödel, p. 191).

VI. If the relation $x_0=\phi(\mathfrak{x}) \epsilon C$, the function $\phi(\mathfrak{x}) \epsilon C$.

For $\phi(\mathfrak{x})=\epsilon x_0[x_0=\phi(\mathfrak{x})]$.

VII. If $\phi(\mathfrak{x})$ is a primitive recursive function, the relation $x_0=\phi(\mathfrak{x}) \epsilon C$.

The proof is by induction with respect to the number of applications of schemas (1) and (2) in the primitive recursive definition of $\phi(\mathfrak{x})$ (see Kleene, Def. 1). First, the proposition $x_0=\phi(\mathfrak{x}) \epsilon C$ holds if $\phi(\mathfrak{x})$ is one of the functions $S(x)$, $C(x)$, $U_i^n(x_1, \cdots, x_n)$, by I and III. Second, if it holds for $\theta(y_1, \cdots, y_m)$, $\chi_1(\mathfrak{x}), \cdots, \chi_m(\mathfrak{x})$, then $\chi_1(\mathfrak{x}), \cdots, \chi_m(\mathfrak{x}) \epsilon C$ by VI, and it holds for $\theta(\chi_1(\mathfrak{x}), \cdots, \chi_m(\mathfrak{x}))$ by I. Third, suppose Gödel, p. 192, 2 holds, where $\psi(x_2, \cdots, x_n)$, $\mu(x_1, \cdots, x_{n+1})$ have the property in question. Following Gödel's discussion, Hilfsatz 1 holds with $n>d$, since d is determined first, and n is any number which satisfies the congruences $n \equiv f_i[\mathrm{mod}(1+(i+1)d)]$, $(i=0, \cdots, k-1)$. Again, $x=[n]_p \epsilon C$. If $P(x_0, \cdots, x_n) \equiv x_0 = \phi(x_1, \cdots, x_n)$, $S(x_0, x_2, \cdots, x_n) \equiv x_0=\psi(x_1, \cdots, x_n)$, $T(x_0, \cdots, x_{n+1}) \equiv x_0=\mu(x_1, \cdots, x_{n+1})$, the relation on page 193 can be restated as follows: $P(x_0, \cdots, x_n) \equiv x_0=[N]_{1+D(x_1+1)}$, where N stands for $\epsilon n[(Ed)[d<n \& \{S([n]_{d+1}, x_2, \cdots, x_n) \& (k)[k<x_1 \rightarrow T([n]_{1+d(k+2)}, k, [n]_{1+d(k+1)}, x_2, \cdots, x_n)]\}]]$ and D stands for $\epsilon d\{S([N]_{d+1}, x_2, \cdots, x_n) \& (k)[k<x_1 \rightarrow T([N]_{1+d(k+2)}, k, [N]_{1+d(k+1)}, x_2, \cdots, x_n)]\}$. It follows that $P(x_0, \cdots, x_n) \epsilon C$.

VIII. Every primitive recursive function ϵC (by VI, VII).

IX. Every recursive function ϵC (by VIII, I, Kleene IV).

X. Every function which ϵC is recursive.

This follows from the recursiveness of $x+y$, $x \cdot y$, δ_y^x and functions obtained from recursive functions by substitution, and Kleene V. Combining IX and X, we have the following result.

XI. The class C of functions is identical with the class of recursive functions.

THE UNIVERSITY OF WISCONSIN

PRODUCTS OF METHODS OF SUMMABILITY*

BY R. P. AGNEW

1. *Introduction.* Let the transforms

$$A: \qquad \sigma_n = \sum_{k=1}^{\infty} a_{nk} s_k,$$

$$B: \qquad \tau_n = \sum_{k=1}^{\infty} b_{nk} s_k,$$

be two regular† methods of summability. Then the A transform $\{\sigma_n\}$ of the B transform $\{\tau_n\}$ of a sequence $\{s_n\}$ is (if it exists) given by

$$(1) \qquad \sigma_n = \sum_{p=1}^{\infty} a_{np}\tau_p = \sum_{p=1}^{\infty}\sum_{k=1}^{\infty} a_{np}b_{pk}s_k.$$

If $\{s_n\}$, bounded or not, is summable B to L so that $\tau_n \to L$, then regularity of A implies that $\{\sigma_n\}$ exists and $\sigma_n \to L$ as $n \to \infty$.

If the sequence $\{s_n\}$ is *bounded*, then the last series in (1) converges absolutely (as a double series) and we can reverse the order of summation to obtain

$$(2) \qquad \sigma_n = \sum_{k=1}^{\infty} \left\{ \sum_{p=1}^{\infty} a_{np}b_{pk} \right\} s_k.$$

The matrix $\|c_{nk}\| \equiv \|\sum a_{np}b_{pk}\|$ of (2) is the ordinary matrix product $\|a_{nk}\|\,\|b_{nk}\|$ and the transformation

$$AB: \qquad \omega_n = \sum_{k=1}^{\infty} c_{nk}s_k$$

is denoted by AB as indicated. We shall show that for regular infinite matrices A, B, it may not be true that $AB \supset B$; and that regularity of A, B, D and equivalence of A and D do not necessarily imply equivalence of AB and DB. We give also related results and applications to kernel transformations.

* Presented to the Society, April 10, 1936.

† The terminology and facts relating to summability which we use are to be found in the expository paper, *Report on topics in the theory of divergent series*, by W. A. Hurwitz, this Bulletin, vol. 28 (1922), pp. 17–36.

2. *Properties of AB.* It is easy to see that AB is regular; in fact if $\{s_n\}$, convergent or not, is a *bounded* sequence summable B to L then we can obtain (2) from (1) and hence conclude that $\{s_n\}$ is summable AB to L.

In case $\|a_{nk}\|$ is row finite (that is, for each n there is an index k_n such that $a_{nk}=0$ when $k>k_n$) the sums over p in (1) and (2) reduce to finite sums; hence we can again obtain (2) from (1) and show that if $\{s_n\}$, bounded or not, is summable B to L, then $\{s_n\}$ is summable AB to L. Therefore if $\|a_{nk}\|$ is row finite, $AB \supset B$.

In case $\|a_{nk}\|$ is not row finite and $\{s_k\}$ is an unbounded sequence summable B to L, then the arguments which we used to justify obtaining (2) from (1) and concluding that $\{s_n\}$ is summable AB to L are void. Hence when $\|a_{nk}\|$ is not row finite, we are unable to prove as above that $AB \supset B$. This inability is fortunate for, as the example of the next section shows, there exist transformations A' and B' (each of which is not only regular but satisfies in addition several conditions of importance in the theory of summability) and a sequence $\{s_n'\}$ summable B' to 0 for which the passage from (1) to (2) is impossible. The sequence $\{s_n'\}$ is in fact not summable $A'B'$.

3. *An Example.* The transformations

$$A': \qquad \sigma_n' = 2^{-1}s_{n+1} + 2^{-2}s_{n+2} + 2^{-3}s_{n+3} + \cdots,$$

$$B': \qquad \tau_n' = (1 - 2^{-n})s_n + 2^{-n}s_{n+1},$$

with matrices $\|a_{nk}'\|$ and $\|b_{nk}'\|$, respectively, are regular. The product matrix $\|c_{nk}'\|$ is easily computed, and the transformation $A'B'$ turns out to be

$$A'B': \quad \omega_n' = (2^{-1} - 2^{-n-2})s_{n+1} + 2^n \sum_{k=n+2}^{\infty} 2^{-k}[1 + 3\cdot 2^{-k}]s_k.$$

The sequence $\{s_n'\}$ defined by $s_1'=1$ and the recursion formula $s_{n+1}'=-(2^n-1)s_n'$, $(n=1, 2, \cdots)$, is summable B' to 0 since substitution of s_n' for s_n in B' gives $\tau_n'=0$ for all n. But $\{s_n'\}$ is not summable $A'B'$; in fact $\lim_{k\to\infty}|2^{-k}[1+3\cdot 2^{-k}]s_k'| = +\infty$, and the series giving ω_n' in terms of s_k therefore diverges for every n when $s_k=s_k'$.

Existence of the sequence $\{s_n'\}$ summable B' but not summable $A'B'$ implies that the convergence field of B' is not con-

tained in the convergence field of $A'B'$, and that the relation $A'B' \supset B'$ is false.

4. *Further Deductions from the Example.* Two methods A and D of summability are called *equivalent* if each sequence evaluated by either A or D is also evaluated to the same value by the other, that is, $A \supset D$ and $D \supset A$. The transformations A' and I (the identity) are equivalent. For A' is regular; and it follows from the definition of A' that $s_{n+1} = 2\sigma_n' - \sigma_{n+1}'$, so that $\sigma_n' \to L$ implies also $s_n \to L$.

Our example shows that regularity of A, B, D together with equivalence of A and D are not sufficient to ensure that AB and DB have the same convergence field; are not sufficient to ensure that $AB \supset DB$; and are not sufficient to ensure equivalence of AB and DB. An example to the contrary is obtained by setting $A = A'$, $B = B'$, and $D = I$.

5. *Kernel Transformations.* The matrix transformation A is a special case of the kernel transformation

$$\mathcal{A}: \qquad \sigma(x) = \int_0^\infty a(x, t)s(t)dt$$

obtained by putting $s(t) = s_k$ when $k-1 \leqq t < k$ and $a(x, t) = a_{nk}$ when $n-1 \leqq x < n$, $k-1 \leqq t < k$ so that $\sigma(x) = \sigma_n$ when $n-1 \leqq x < n$. The $\mathcal{A}$ transform of a $\mathcal{B}$ transform of a function $s(t)$ is (if it exists) given by

$$\sigma(x) = \int_0^\infty d\alpha \int_0^\infty a(x, \alpha)b(\alpha, t)s(t)dt.$$

Our example illustrates the fact that, even though $\mathcal{A}$ and $\mathcal{B}$ be regular and $s(t)$ be summable $\mathcal{B}$, the formal inversion of order of integration to obtain

$$(3) \qquad \sigma(x) = \int_0^\infty \left\{ \int_0^\infty a(x, \alpha)b(\alpha, t)d\alpha \right\} s(t)dt$$

may be unjustified; and that, if $\mathcal{AB}$ denotes the kernel transformation (3), it may in fact fail to be true that $\mathcal{AB} \supset \mathcal{B}$.

CORNELL UNIVERSITY

A GENERALIZATION OF A CYCLOTOMIC FORMULA*

BY H. S. GRANT

1. *Introduction.* Jacobi stated without proof† the following cyclotomic formula

$$F(-1)\cdot F(\alpha^2) = \alpha^{2m}F(\alpha)\cdot F(-\alpha),$$

where

$$F(\alpha) = x + \alpha x^g + \alpha^2 x^{g^2} + \cdots + \alpha^{q-2}x^{g^{q-2}},$$

q is an odd prime, g a primitive root, mod q, $g^m \equiv 2$, mod q, $x^q = 1 (x \neq 1)$, $\alpha^{q-1} = 1 (\alpha \neq 1)$. This relation is essentially one involving Lagrange resolvent functions, and ultimately reduces to one connecting two Jacobi ψ-functions. The former have been generalized by L. Stickelberger,‡ and the latter by H. H. Mitchell.§

It is the purpose of this paper to generalize Jacobi's formula to the case $q^t \equiv 1$, mod n, q an odd prime, t any exponent for which the congruence holds, n even. If we take $t = 1, n = q-1$, the relation stated above then follows as a special case. Before proceeding further, the reader is strongly advised to refer to Mitchell's paper mentioned above, frequent use of which is made in what follows.

2. *Characteristic Properties of the Generalized Function.* If $s(x) = \sum_{i=0}^{t-1} a_i x^i$, a_i reduced, mod q, q prime, $s(q)$ will represent a complete residue system, mod q^t. We interpret $s(x)$ as the marks of a Galois field of order q^t. Let ϵ denote a primitive nth root of unity, where $q^t \equiv 1$, mod n, and τ a primitive q^tth root of unity. We define

$$(\epsilon^\lambda, \tau) = \sum_s \epsilon^{\lambda \operatorname{ind} s(x)} \tau^{s(q)},$$

the summation being taken over all marks excepting 0, and the

* Presented to the Society, September 13, 1935.

† Journal für Mathematik, vol. 30 (1846), p. 167.

‡ Mathematische Annalen, vol. 37 (1890), pp. 321–367.

§ Transactions of this Society, vol. 17 (1916), pp. 165–177.

index being taken with respect to a primitive root $g(x)$ in the Galois field. We set $q^t-1=kn$. For convenience of reference, we list the following characteristic properties of the function (ϵ^λ, τ).

(1) $$(1, \tau) = -1.$$

(2) $$(\epsilon^\lambda, \tau)(\epsilon^{-\lambda}, \tau) = (-1)^{k\lambda} q^t, \qquad q \text{ odd},$$
$$= q^t, \ q = 2, \text{ provided } n \nmid \lambda.$$

(3) $$\frac{(\epsilon^\lambda, \tau)(\epsilon^{-\mu}, \tau)}{(\epsilon^{\lambda+\mu}, \tau)} = \Psi_{\lambda,\mu}(\epsilon),$$

where

$$\Psi_{\lambda,\mu}(\epsilon) = \sum_s \epsilon^{\mu \text{ ind } s - (\lambda+\mu) \text{ ind } (s+1)}, \qquad (n \nmid \lambda + \mu),$$

s goes over all the marks of our Galois field excepting 0 and -1 if q is odd, and 0 and 1 if q is 2.*

(4) (a) $$\Psi_{\lambda,\mu}(\epsilon)\Psi_{\lambda,\mu}(\epsilon^{-1}) = q^t,$$

(b) $$\Psi_{\lambda,\mu}(\epsilon^q) = \Psi_{\lambda,\mu}(\epsilon),$$

where

$$\lambda, \mu, \lambda + \mu \not\equiv 0 \mod n.$$

(5) Let $q_i = q(\epsilon^{i'})$, where $ii' \equiv 1$, mod n, and q_i is any prime ideal factor of q in the cyclotomic number-realm $k(\epsilon)$. Further, let i assume the $\phi(n)/t_1$ values prime to n such that the quotient of no two of them is congruent, mod n, to a power of q, t_1 being the exponent to which q belongs, mod n. If $g^k \equiv \epsilon$, mod $q(\epsilon)$, $g = g(\epsilon)$, then the principal ideal satisfies the relation

$$[\Psi_{\lambda,\mu}(\epsilon)] = \prod_i q_i^{m_i},$$

m_i denoting the number of sums

$$|-\lambda i q^{t-j}| + |-\mu i q^{t-j}|, \qquad (j = 0, 1, \cdots, t-1),$$

whose values exceed n, $|x|$ being the least positive residue of x, mod n, and $\lambda, \mu, \lambda+\mu \not\equiv 0$, mod n.†

* Properties (1), (2), and (3) are analogous to those for the Lagrange function. Compare H. Weber, *Lehrbuch der Algebra*, 2nd ed., vol. 1, 1899, pp. 611–612.

† See H. H. Mitchell, loc. cit., for properties (4) and (5), particularly pages 168, 169, and 173.

Properties (1) and (2) show that $(\epsilon^\lambda, \tau) \neq 0$ for any λ. Taking n as even, so that q must be an odd prime, we shall prove that

$$(A) \qquad (\epsilon^{n/2}, \tau)(\epsilon^{2\lambda}, \tau) = \epsilon^{2m\lambda}(\epsilon^\lambda, \tau)(\epsilon^{\lambda+n/2}, \tau),$$

where $0<\lambda<n$, $g^m \equiv 2$, mod $q(\epsilon)$, $g=g(\epsilon)$. As remarked in the introduction, this reduces to the Jacobi formula when $n=q-1$, q an odd prime, and $t=1$. We have replaced α by ϵ^λ, and x by τ.

3. *The Cases* $\lambda \equiv \pm n/4$, mod n. In either of the cases $\lambda \equiv \pm n/4$, mod n, (A) becomes by virtue of (2), and since $\epsilon^{n/2} = -1$,

$$(-1)^{k\cdot n/2} q^t = (-1)^m (-1)^{k\cdot n/4} q^t,$$

that is,

$$(B) \qquad 1 = (-1)^m (-1)^{kn/4}.$$

Since $4 \mid n$, i is a number of $k(\epsilon)$. Now

$$g^{kn/2} + 1 = (g^{kn/4} - i)(g^{kn/4} + i) \equiv 0, \text{ mod } q(\epsilon),$$

whence ind $i = \pm kn/4$. But $2 = i(1-i)^7$, therefore ind $2 \equiv$ ind i $+2$ ind $(1-i)$, mod kn, and consequently ind 2 and ind i are both even or both odd, which establishes (B), since ind $2 = m$.

Excepting the above values of λ, (A) becomes from property (3),

$$(C) \qquad \Psi_{n/2,2\lambda}(\epsilon) = \epsilon^{2m\lambda} \Psi_{\lambda,\lambda+n/2}(\epsilon).$$

Equation (C) is evidently true for $\lambda = n/2$, and it is only necessary to prove it for $0<\lambda<n/2$. For, if $\lambda = n/2+a$, $0<a<n/2$,

$$\Psi_{n/2,2\lambda}(\epsilon) = \Psi_{n/2,2a}(\epsilon)$$

$$\Psi_{\lambda,\lambda+n/2}(\epsilon) = \Psi_{n/2+a,a}(\epsilon) = \Psi_{a,a+n/2}(\epsilon).$$

In what follows, we assume $g^k \equiv \epsilon$, mod $q(\epsilon)$, a restriction that we will remove later.

4. *A Relation between the* Ψ*-Functions.* Using (5), we have

$$[\Psi_{n/2,2\lambda}(\epsilon)] = [\Psi_{\lambda,\lambda+n/2}(\epsilon)],$$

whence

$$\Psi_{n/2,2\lambda}(\epsilon) = E(\epsilon)\Psi_{\lambda,\lambda+n/2}(\epsilon),$$

where $E(\epsilon)$ is a unit. For, since iq^{t-j} is odd,

$$|(-n/2)iq^{t-j}| + |-2\lambda iq^{t-j}| = n/2 + 2|-\lambda iq^{t-j}|$$
$$= |-\lambda iq^{t-j}| + |-(\lambda + n/2)iq^{t-j}|, \quad (j = 0, 1, \cdots, t-1),$$

when $|-\lambda iq^{t-j}| < n/2$, and,

$$|(-n/2)iq^{t-j}| + |-2\lambda iq^{t-j}| = n/2 + 2|-\lambda iq^{t-j}| - n$$
$$= |-\lambda iq^{t-j}| + |-(\lambda + n/2)iq^{t-j}|,$$

when $|-\lambda iq^{t-j}| > n/2$. Replacing ϵ by ϵ^{-1}, above, we have

$$\Psi_{n/2,2\lambda}(\epsilon^{-1}) = E(\epsilon^{-1})\Psi_{\lambda,\lambda+n/2}(\epsilon^{-1}).$$

Making use of (4a), we obtain $E(\epsilon)E(\epsilon^{-1}) = 1$, whence $E(\epsilon)$ is a root of unity, say ϵ^b.* Now we have

$$\Psi_{n/2,2\lambda}(\epsilon) = \epsilon^b\Psi_{\lambda,\lambda+n/2}(\epsilon).$$

Since $g^k \equiv \epsilon$, mod $q(\epsilon)$, we have at once

$$\Psi_{n/2,2\lambda}(g^k) \equiv g^{kb}\Psi_{\lambda,\lambda+n/2}(g^k), \text{ mod } q(\epsilon).$$

Referring back to the definition of the Ψ-function in §2, we readily see that this congruence reduces to

$$\sum_x g^{2k\lambda x}(g^x + 1)^{k\nu} \equiv g^{kb}\sum_x g^{k\lambda x}(g^x + 1)^{k\nu}, \text{ mod } q(\epsilon),$$

where $2\lambda + n/2 + \nu \equiv 0$, mod n, and x goes through all values $0, 1, \cdots, kn-1$ excepting $kn/2$. Thus

$$g^{kb} \equiv \frac{\sum_x g^{2k\lambda x}(g^x + 1)^{k\nu}}{\sum_x g^{k\lambda x}(g^x + 1)^{k\nu}}, \text{ mod } q(\epsilon),$$

and we proceed to determine what the right-hand member of this congruence reduces to as a function of g, a primitive (kn)th root of unity.

5. *The Determination of b.* Since $g^{kn/2} = -1$, we may let x take all values $0, 1, \cdots, kn-1$. Now

* See D. Hilbert, *Gesammelte Abhandlungen*, vol. 1, 1932, Theorem 48, §21; R. Fricke, *Lehrbuch der Algebra*, vol. 3, 1928, p. 200.

$$\sum_{x=0}^{kn-1} g^{2k\lambda x}(g^x+1)^{k\nu} = \sum_{x=0}^{kn-1} g^{2k\lambda x} \sum_{h=0}^{k\nu} C_{k\nu,h} g^{(k\nu-h)x}$$

$$= \sum_{h=0}^{k\nu} C_{k\nu,h} \sum_{x=0}^{kn-1} g^{(2k\lambda+k\nu-h)x},$$

where $C_{c,d}$ is the binomial coefficient $c!/d!(c-d)!$. But

$$\sum_{x=0}^{kn-1} g^{lx} = \frac{(g^l)^{kn}-1}{g^l-1} = 0 \text{ or } kn,$$

according as kn does not or does divide l. Taking $0<\nu<n$, we have, since $0<\lambda<n/2$, $\nu=n/2-2\lambda$ or $3n/2-2\lambda$ according as $\lambda<n/4$ or $\lambda>n/4$. In the first case, $2k\lambda+k\nu-h \leqq kn/2$, and, in the second, $2k\lambda+k\nu-h=3kn/2-h=kn$, when $h=kn/2$. From these considerations, we have

$$\sum_{x=0}^{kn-1} g^{2k\lambda x}(g^x+1)^{k\nu} = (kn)C_{3kn/2-2k\lambda,\, kn/2},$$

provided $n/4<\lambda<n/2$.*

Similarly

$$\sum_{x=0}^{kn-1} g^{k\lambda x}(g^x+1)^{k\nu} = (kn)C_{3kn/2-2k\lambda,\, kn/2-k\lambda},$$

under the same restrictions for λ. We now have

$$\frac{\sum_{x=0}^{kn-1} g^{2k\lambda x}(g^x+1)^{k\nu}}{\sum_{x=0}^{kn-1} g^{k\lambda x}(g^x+1)^{k\nu}} = \frac{(kn/2-k\lambda)!(kn-k\lambda)!}{(kn/2)!(kn-2k\lambda)!},$$

provided $n/4<\lambda<n/2$. This last quotient is

$$\frac{(kn-k\lambda)(kn-k\lambda-1)\cdots(kn-2k\lambda+1)}{(kn/2)(kn/2-1)\cdots(kn/2-k\lambda+1)}$$

$$= \frac{2^{k\lambda}(kn-k\lambda)(kn-k\lambda-1)\cdots(kn-2k\lambda+1)}{(kn)(kn-2)\cdots(kn-2k\lambda+2)}$$

$$= \frac{2^{k\lambda}(q^t-2k\lambda)(q^t-2k\lambda+1)\cdots(q^t-k\lambda-1)}{(q^t-1)(q^t-3)\cdots(q^t-2k\lambda+1)}$$

* Compare H. Weber, loc. cit., pp. 620–621.

$$= 2^{k\lambda} \prod_{i=0}^{k\lambda-1} \left[\frac{q^t - (2k\lambda - i)}{q^t - (2i+1)} \right].$$

Now let

$$q^t - (2k\lambda - i) = q^{s_i}(q^{t-s_i} - k_i),$$
$$q^t - (2i+1) = q^{t_i}(q^{t-t_i} - l_i),$$

so that both k_i and l_i are prime to q, and s_i, $t_i < t$, since $2k\lambda < q^t - 1$. Then our quotient becomes

$$2^{k\lambda} \prod_{i=0}^{k\lambda-1} \frac{q^{s_i}(q^{t-s_i} - k_i)}{q^{t_i}(q^{t-t_i} - l_i)}.$$

But

$$\prod_{i=0}^{k\lambda-1} \frac{q^{s_i} k_i}{q^{t_i} l_i} = \frac{(2k\lambda)(2k\lambda - 1) \cdots (k\lambda + 1)}{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2k\lambda - 1)}$$
$$= \frac{(2k\lambda)!}{[1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2k\lambda - 1)](k\lambda)!} = 2^{k\lambda}.$$

Therefore, since q is an odd prime, and k_i, l_i are prime to q, we have $\prod_{i=0}^{k\lambda-1} q^{s_i} = \prod_{i=0}^{k\lambda-1} q^{t_i}$. Our quotient is now

$$2^{k\lambda} \prod_{i=0}^{k\lambda-1} \frac{(q^{t-s_i} - k_i)}{(q^{t-t_i} - l_i)}$$

which is congruent to $2^{k\lambda} \prod_{i=0}^{k\lambda-1} k_i / l_i = 2^{2k\lambda}$, mod $q(\epsilon)$. Since $2 \equiv g^m$, mod $q(\epsilon)$, it follows from the previous section that

$$g^{kb} \equiv g^{2km\lambda}, \text{ mod } q(\epsilon),$$

whence

$$kb \equiv 2km\lambda, \text{ mod } kn,$$
$$b \equiv 2m\lambda, \text{ mod } n.$$

6. *Removal of the Restrictions.* Equation (C) has been established when $n/4 < \lambda < n/2$, and $g^k \equiv \epsilon$, mod $q(\epsilon)$. Replacing ϵ by ϵ^{-1} in (C), we have

$$\Psi_{n/2,2\lambda}(\epsilon^{-1}) = \epsilon^{-2m\lambda} \Psi_{\lambda,\lambda+n/2}(\epsilon^{-1}), \qquad (n/4 < \lambda < n/2),$$

or

$$\Psi_{n/2,-2\lambda}(\epsilon) = \epsilon^{-2m\lambda}\Psi_{-\lambda,-\lambda+n/2}(\epsilon),$$

that is,

$$\Psi_{n/2,2\mu}(\epsilon) = \epsilon^{2m\mu}\Psi_{\mu,\mu+n/2}(\epsilon), \qquad (-n/2 < \mu < -n/4).$$

If $\mu = \nu - n/2$, we have

$$\Psi_{n/2,2\nu}(\epsilon) = \epsilon^{2m\nu}\Psi_{\nu,\nu+n/2}(\epsilon), \qquad (0 < \nu < n/4).$$

To remove the restriction on g, we introduce a simple change of notation, writing ((3), §2)

$$\Psi_{a,b}(\epsilon, g) = \sum_{s} \epsilon^{b \operatorname{ind}_g s - (a+b) \operatorname{ind}_g (s+1)}.$$

Referring to (C), we wish to show

(C′) $$\Psi_{n/2,2\lambda}(\epsilon, G) = \epsilon^{2M\lambda}\Psi_{\lambda,\lambda+n/2}(\epsilon, G),$$

where $0 < \lambda < n$, $G^M \equiv 2$, mod $q(\epsilon)$, G being any primitive root of our Galois field. Let $G \equiv g^s$, mod $q(\epsilon)$, so that ind $_g s \equiv z$ ind $_G s$, mod kn. Then

$$\Psi_{a,b}(\epsilon^{z'}, g) = \Psi_{a,b}(\epsilon, G),$$

where $zz' \equiv 1$, mod kn. Replacing ϵ by $\epsilon^{z'}$ in (C), we have

$$\Psi_{n/2,2\lambda}(\epsilon^{z'}, g) = \epsilon^{2m\lambda z'}\Psi_{\lambda,\lambda+n/2}(\epsilon^{z'}, g),$$

or

$$\Psi_{n/2,2\lambda}(\epsilon, G) = \epsilon^{2m\lambda z'}\Psi_{\lambda,\lambda+n/2}(\epsilon, G).$$

Writing M for mz', we have

$$G^M = G^{mz'} \equiv g^{mzz'} \equiv g^m \equiv 2, \text{ mod } q(\epsilon),$$

and (C′) is established.

RUTGERS UNIVERSITY

ARITHMETICAL CONSEQUENCES OF A TRIGONOMETRIC IDENTITY

BY E. T. BELL

1. *Identities.* The formulas for the product of s sines, t cosines, or s sines and t cosines, give immediate elementary proofs concerning representations of numbers in certain forms of degrees s, t, $s+t$. Here we consider s sines, where $s>1$. Let us write

$$\psi_n(x_1, \cdots, x_s) \equiv \sum e_2 \cdots e_s(x_1 + e_2x_2 + \cdots + e_sx_s)^n,$$

where $\sum$ refers to the 2^{s-1} possible sets $(e_2, \cdots, e_s)$, $e_j = \pm 1$, $(j=2, \cdots, s)$. Then, for $t>0$,

$$2^{2t-1}(-1)^t \prod_{j=1}^{2t} \sin x_j\theta = \cos \psi(x_1, \cdots, x_{2t})\theta,$$

$$2^{2t}(-1)^t \prod_{j=1}^{2t+1} \sin x_j\theta = \sin \psi(x_1, \cdots, x_{2t+1})\theta,$$

in which, after expansion of the (symbolic) cos, sin on the right, $\psi^n(\ )$ is to be replaced by $\psi_n(\ )$. Such expansions were discussed in detail in a previous paper.*

The results of equating coefficients of θ^{2t}, θ^{2t+1} in these can be combined at once into the single identity

$$s!2^{s-1}x_1 \cdots x_s = \psi_s(x_1, \cdots, x_s). \tag{1}$$

For $s=3$, (1) is due to Gauss, for $s>1$, to Tardy, who proved a slightly different form of (1) otherwise.† In the same way we see that

$$\psi_n(x_1, \cdots, x_s) = 0, \qquad n < s. \tag{2}$$

In (1) let $x_1=x$, $x_j=1$ $(j>1)$. If precisely p of $e_2, \cdots, e_s$ are $+1$, $e_2+\cdots+e_s=2p+1-s$, $e_2 \cdots e_s=(-1)^{s-1-p}$. The p can be chosen in ${}_{s-1}C_p$ ways. Hence we have

$$(-1)^{s-1}s!2^{s-1}x = \sum_{p=0}^{s-1} (-1)^p {}_{s-1}C_p(x + 2p + 1 - s)^s. \tag{3}$$

* Transactions of this Society, vol. 38(1926), pp. 129–148.

† Annali di Scienze Matematische e Fisiche, vol. 2(1851), pp. 287–291.

In (1) let $x_1=x_2=x$, $x_j=1$ $(j>2)$. Separating the terms according as $e=1$ or -1, and proceeding as before, we get

$$(4)\quad (-1)^s s!2^{s-1}x^2 = \sum_{p=0}^{s-2}(-1)^p {}_{s-2}C_p[(2x+2p+2-s)^s - (2p+2-s)^s].$$

Similarly,

$$(5)\quad (-1)^s s!2^{s-1}x^3 = \sum_{p=0}^{s-3}(-1)^p {}_{s-3}C_p[2(x+2p+3-s)^s - (-x+2p+3-s)^s - (3x+2p+3-s)^s].$$

The general formula of the same sort for x^n, $n>3$, is easily obtained by the methods of the first paper cited, on using the expansions for powers of sines in terms of multiple angles.

From (3)–(5), by differentiation with respect to x, we obtain

$$(6)\quad \sum_{p=0}^{s-1}(-1)^p {}_{s-1}C_p(x+2p+1-s)^{s-j} = 0, \qquad (j>1);$$

$$(7)\quad \sum_{p=0}^{s-1}(-1)^p {}_{s-2}C_p(2x+2p+2-s)^{s-j} = 0, \qquad (j>2);$$

$$(8)\quad \sum_{p=0}^{s-1}(-1)^p {}_{s-3}C_p[2(x+2p+3-s)^{s-j} - (-x+2p+3-s)^{s-j} - (3x+2p+3-s)^{s-j}] = 0, \qquad (j>3),$$

valid for all x.

2. *Theorems on Representations.* (I) Let α be any integer in an algebraic number field K of (arbitrary) degree k. Then

$$(9)\quad s!2^{s-1}\alpha = e_1\alpha_1^s + \cdots + e_n\alpha_n^s, \qquad (n \leqq 2^{s-1}),$$

$$(-1)^{s-1}s!2^{s-1}\alpha = \sum_{p=0}^{s-1}(-1)^p {}_{s-1}C_p\beta_p^s,$$

where the α's, β's are integers in K. These follow at once from (1), (3). In the first we may take $\alpha=\gamma_1\cdots\gamma_s$, $x_j=\gamma_j$, where the γ's are integers in K. If $k=1$, the α's are rational integers, and if t is the least integer such that τ is represented in the form

$e_1\alpha_1^s + \cdots + e_t\alpha_t^s$, all $\alpha \equiv \tau \bmod s!2^{n-1}$ are represented in (9) with $n \leqq 2^{s-1}+t$.

(II) Since every (rational) integer m is a sum of four (rational integer) squares, it follows from (5) that

$$(-1)^s s!2^{s-1}m + 4\sum_{p=0}^{s-2} {}_{s-2}C_p(2p+2-s)^s$$

is a sum of 4 values of

$$\sum_{p=0}^{s-2} (-1)^p {}_{s-2}C_p m_p^s,$$

where the m's are integers.

Similarly, from (5), every $(-1)s!2^{s-1}m$ is a sum of 9 values of

$$\sum_{p=0}^{s-3} (-1)^p {}_{s-3}C_p(2m_p^s - n_p^s - r_p^s),$$

where m, n, p are integers. Theorems of this sort can be continued indefinitely.

3. *A Rational Canonical.* Let $P \equiv P(y_1, \cdots, y_n)$ be a polynomial (not necessarily homogeneous) of degree s in $y_1, \cdots, y_n$, containing precisely p terms. Then immediately from (1),

$$s!2^{s-1}P = \sum_{j=1}^{h} A_j Y_j^s, \qquad h \leqq 2^{s-1}p,$$

where the A's are linear in the coefficients of P, and the Y's are linear in $y_1, \cdots, y_n$, both with rational integer coefficients.

4. *Equal Sums of Like Powers.* From (2) we have an infinity of solutions of

$$a_1^n + \cdots + a_t^n = b_1^n + \cdots + b_t^n, \qquad t = 2^{s-2},$$
$$(n = 0, 1, \cdots, s-1),$$

in integers a, b. Similarly from (6)–(8). Thus from (6), for example,

$$\sum_{p=0}^{s-1} (-1)^p {}_{s-1}C_p(x+2p+1-s)^{s-i}$$
$$= \sum_{p=0}^{s-1} (-1)^p {}_{s-1}C_p(y+2p+1-s)^{s-i}$$

for $0<j\leqq s$, and x, y arbitrary. Hence, for the same j,

$$\sum_{p=0}^{2p\leqq s-1} {}_{s-1}C_{2p}(x+4p+1-s)^{s-j} + \sum_{p=0}^{2p\leqq s-2} {}_{s-1}C_{2p+1}(y+4p+3-s)^{s-j} = \sum_{p=0}^{2p\leqq s-2} {}_{s-1}C_{2p+1}(x+4p+3-s)^{s-j} + \sum_{p=0}^{2p\leqq s-1} {}_{s-1}C_{2p}(y+4p+1-s)^{s-j}.$$

One term on each side can be made to vanish by suitably choosing x, y. Thus we have a solution of

$$a_1^n + \cdots + a_u^n = b_1^n + \cdots + b_u^n, \qquad u = 2^{s-2} - 1, \quad (n = 0, \cdots, s-1).$$

Similar devices give corresponding results for any $u\leqq 2^{s-2}$, and solutions containing parameters can also be given.

California Institute of Technology

A CORRECTION IN THE LIST OF PRIMES

BY D. N. LEHMER

My attention has been called by Andr. W. Mund of Basel, Switzerland, to a second error in the *List of Primes* published for me by the Carnegie Institution of Washington in 1914. The number 854651 listed in those tables is not a prime and should read 854647. The error is due to an error hitherto undiscovered in Burckhardt's Tables of Divisors, in which an entry of 7 has slipped up one line. The error does not occur in my *Factor Tables*, and was introduced into the list from Burckhardt's tables, which were more convenient to read than the Carnegie tables.

All users of these tables should insert this correction. It is the second error to be discovered so far. (See this Bulletin, vol. 38 (1932), p. 902.)

The University of California

DEFINITION OF SUBSTITUTION

BY W. V. QUINE*

1. *Basis.* The *elements* of this study, denoted by italic capitals, comprise *atoms*, at least two and perhaps infinite in number, and all finite *sequences* of such atoms. (The atoms are interpretable as signs, for example, and the sequences as rows of signs.) Thus each element E is composed successively of possibly duplicative atoms $A_1, A_2, \cdots$, and A_m, for some positive integer m, called the *length* of E; and an element F composed successively of atoms B_1 to B_n will be identical with E if and only if $m=n$ and $A_i=B_i$ for each i to m.

Further terminology is self-explanatory. Thus we may speak of the kth *place* of an element; this, in the case of E above, is occupied by the atom A_k. We may speak of one element as *occurring in* another (as a connected segment thereof), and more particularly as occurring *initially*, *internally*, or *terminally* therein; of two elements as occurring *overlapped* in a third; of the number of occurrences of one element in another; and so on.

Juxtaposition will be used to express that binary operation of *concatenation* whereby any elements E and F, composed as above, are put end to end to form that element EF which is composed successively of the atoms $A_1, A_2, \cdots, A_m, B_1, B_2, \cdots$, and B_n. The element E is itself describable, in terms of concatenation of its atoms, as $A_1A_2 \cdots A_m$; parentheses are suppressed, as here, in view of the obvious associativity of concatenation.

It is clear that the length of EF, for any E and F, exceeds the lengths of E and F and equals their sum; also that E occurs initially and F terminally in EF, while EF occurs neither in E nor in F; also that atoms are of length 1, and that an element G is an atom if and only if there are no elements E and F such that $G=EF$.

2. *Substitution.* The purpose of this paper is a formal definition of *substitution* in terms exclusively of concatenation and the following elementary logical devices: identity, applied to

* Society of Fellows, Harvard University.

elements; the truth functions; and quantification with respect to elements. The notation will be as in *Principia Mathematica*: the sign '=' for identity, the signs '$\sim$', '$\supset$', $\cdots$, for the truth functions, and prefixes of the forms '(X)' and '$(\exists X)$' for quantification.

The proposition to be formulated is expressible verbally thus: W is the result of substituting X for Y throughout Z; briefly, $sub(W, X, Y, Z)$. When the elements are interpreted as signs and rows of signs, the notion under consideration is the notational substitution which figures so prominently in metamathematics.

In the general form in which substitution is here conceived, its formulation is complicated by the fact that the element Y for which substitution is made need not be an atom and hence may have overlapping occurrences in Z. Obviously we cannot in general replace each of two overlapping occurrences of Y by X, since replacement of one occurrence will mutilate the other occurrence. To this extent the notion of substitution is ambiguous. The ambiguity is resolved by stipulating that in case of overlapping occurrences left is to prevail over right; thus the result of substituting X for TT in TTT is to be XT rather than TX. The result of substituting X for Y throughout Z is then describable, in general, as the result Z' of putting X for each of these occurrences of Y in Z: the first (left-most); the first which begins after the end of that first; the first which begins after the end of this second; and so on. In the trivial case where Y does not occur in Z, Z' is of course Z.

3. *Formal Definitions.* The following abbreviations are adopted:

D1. $\quad U \textit{ init } V \mathrel{.=_{df}} U = V \mathrel{.\vee:} (\exists T).\ UT = V.$

D2. $\quad U \textit{ in } V \mathrel{.=_{df}} U \textit{ init } V \mathrel{.\vee:} (\exists T).\ TU \textit{ init } V.$

D3. $\quad U \sim \textit{in } V \mathrel{.=_{df}} \sim.\ U \textit{ in } V.$

D4. $\quad \Theta(U, V, M, N) \mathrel{.=_{df}} .\ MUMVM \textit{ in } N \mathrel{.} M \sim \textit{in } UV.$

D5. $\quad sub1(U, X, Y, V) \mathrel{.=_{df}} : U$

$$= X \mathrel{.} V = Y \mathrel{.\vee:} (\exists T).\ U = TX \mathrel{.} V = TY : \sim(\exists S).\ YS \textit{ in } V.$$

Obviously 'U *init* V' may be read 'U occurs initially in V', and

'*U in V*' may be read '*U* occurs in *V*'. Again, '*sub* 1(*U*, *X*, *Y*, *V*)' tells us that *Y* occurs in *V* terminally and only so and that *U* is the result of putting *X* for *Y* in *V*; this is seen as follows. For *Y* to occur terminally in *V* it is necessary and sufficient that either $V = Y$ or $(\exists T) \cdot V = TY$. Where $V = Y$ it is clear further that *Y* does not occur in *V* otherwise than terminally; where $(\exists T) \cdot V = TY$, on the other hand, in order that *Y* not occur in *V* otherwise than terminally it is obviously necessary and sufficient to add that $\sim(\exists S) \cdot YS$ *in* *V*. In general, therefore, for *Y* to occur in *V* terminally and only so it is necessary and sufficient that

$$V = Y \;.\vee: (\exists T).\; V = TY : \sim (\exists S).\; YS \textit{ in } V.$$

Now if *U* is the result of putting *X* for *Y* in *V*, *U* will be *X* or *TX* according as *V* is *Y* or *TY*. D5 thus yields the described meaning.

The definition of substitution follows:

D6. $$\begin{aligned} &sub(W, X, Y, Z) \;.=_{df}::: .\; Y \sim in\, Z \;.\; W = Z \;.\vee ::: . \\ &(\exists G)(\exists H)::: (M)(N)::.\; (U)(V):: sub1(U, X, Y, V).\supset \\ &:.\; V \textit{ init } Z \;.\supset .\; \Theta(U, V, M, N):.\; (S)(T):\Theta(S, T, M, N) \\ &.\; TV \textit{ init } Z \;.\supset .\; \Theta(SU, TV, M, N) :: \supset .\; \Theta(G, H, M, N) \\ &::: W = G \;.\; Z = H \;.\vee: (\exists K).\; Y \sim in\, K \;.\; W = GK \\ &.\; Z = HK. \end{aligned}$$

When abbreviations introduced by D1–D5 are eliminated in favor of their definientia, the definiens in D6 is seen to involve only concatenation and the elementary logical devices mentioned in §2.

4. *Demonstrandum.* It remains to show that D6 yields substitution in the sense of §2; that is, that *sub*(*W*, *X*, *Y*, *Z*), in the sense of D6, if and only if *W* is *Z'* as of §2.

Supposing *W*, *X*, *Y*, and *Z* given as constants, we define as follows:

Dt1. $$\begin{aligned} &\Phi(M, N) \cdot =_{df}:: (U)(V):: sub1(U, X, Y, V) \cdot \supset :\cdot \\ &V \textit{ init } Z \cdot \supset \cdot \Theta(U, V, M, N) :\cdot (S)(T):\Theta(S, T, M, N) \\ &\cdot\; TV \textit{ init } Z \cdot \supset \cdot \Theta(SU, TV, M, N). \end{aligned}$$

Dt2. $\Psi(F, G, H) \cdot =_{df} : \cdot (M)(N) : \Phi(M, N) \cdot \supset \cdot \Theta(G, H, M, N)$
$: \cdot F = G \cdot Z = H \cdot \vee : (\exists K) \cdot Y \sim in\ K \cdot F = GK$
$\cdot Z = HK.$

By §1, $(U)(V) \cdot XUXVX \sim in\ X$; by D4, then, $(U)(V) \cdot \sim\Theta(U, V, X, X)$, so that

(1) $(U)(V) : \cdot V\ init\ Z \cdot \supset \cdot \Theta(U, V, X, X) : \equiv \cdot \sim \cdot V\ init\ Z,$

(2) $(G)(H) : \cdot \Phi(X, X) \cdot \supset \cdot \Theta(G, H, X, X) : \equiv \cdot \sim \Phi(X, X),$

and, trivially,

(3) $(U)(V)(S)(T) : \Theta(S, T, X, X) \cdot TV\ init\ Z \cdot \supset \cdot \Theta(SU, TV, X, X).$

By Dt1, (1), and (3),

$\Phi(X, X) \cdot \equiv : (U)(V) : sub1(U, X, Y, V) \cdot \supset \cdot \sim \cdot V\ init\ Z,$

whence $\sim\Phi(X, X) \cdot \supset \cdot (\exists U)(\exists V) \cdot sub1(U, X, Y, V) \cdot V\ init\ Z,$ and therefore, by D5,

$\sim \Phi(X, X) \cdot \supset : \cdot (\exists V) : \cdot V = Y \cdot \vee : (\exists T) \cdot V = TY : \cdot V\ init\ Z,$

that is, $\sim\Phi(X, X) \cdot \supset : Y\ init\ Z \cdot \vee : (\exists T) \cdot TY\ init\ Z,$ which is to say, by D2,

(4) $\sim \Phi(X, X) \cdot \supset \cdot Y\ in\ Z.$

By Dt2, $(G)(H) : \cdot \Psi(W, G, H) \cdot \supset : \Phi(X, X) \cdot \supset \cdot \Theta(G, H, X, X)$ whence, by (2) and (4),

$(G)(H) : \Psi(W, G, H) \cdot \supset \cdot Y\ in\ Z,$

that is, $(\exists G)(\exists H) \cdot \Psi(W, G, H) \cdot \supset \cdot Y\ in\ Z$, or, equivalently,

(5) $(\exists G)(\exists H) \cdot \Psi(W, G, H) \cdot \equiv : Y\ in\ Z : (\exists G)(\exists H) \cdot \Psi(W, G, H).$

If Y does not occur in Z, then, by §2, Z' is Z. Hence

(6) $Y \sim in\ Z \cdot W = Z \cdot \equiv \cdot Y \sim in\ Z \cdot W = Z'.$

By D6, Dt1, and Dt2,

$sub(W, X, Y, Z) \cdot \equiv : Y \sim in\ Z \cdot W = Z \cdot \vee : (\exists G)(\exists H) \cdot \Psi(W, G, H).$

Hence, by (5) and (6),

$$(7)\qquad \begin{aligned} sub(W, X, Y, Z) \cdot \equiv : Y \sim \varepsilon Z \cdot W = Z' \cdot \vee : Y \varepsilon Z \\ : (\exists G)(\exists H) \cdot \Psi(W, G, H). \end{aligned}$$

Now if we can prove that

$$(I)\qquad Y \varepsilon Z \cdot \supset : (\exists G)(\exists H) \cdot \Psi(W, G, H) \cdot \equiv \cdot W = Z',$$

so that $Y \varepsilon Z : (\exists G)(\exists H) \cdot \Psi(W, G, H) : \equiv \cdot Y \varepsilon Z \cdot W = Z'$, then from (7) we shall have

$$sub(W, X, Y, Z) \cdot \equiv \cdot Y \sim \varepsilon Z \cdot W = Z' \cdot \vee \cdot Y \varepsilon Z \cdot W = Z',$$

that is, $sub\ (W, X, Y, Z) \cdot \equiv \cdot W = Z'$ which was to be proved. It thus remains only to establish (I).

5. *Proof of* (I). Given that Y occurs in Z, it is to be proved that

$$(\exists G)(\exists H) \cdot \Psi(W, G, H) \cdot \equiv \cdot W = Z'.$$

Consider the following segments Z_i of Z; Z_1 extends from the beginning of Z to the end of the first occurrence of Y in Z; Z_2 extends from the beginning of Z^1 to the end of the first occurrence of Y in Z^1, where Z^1 is Z deprived of its initial segment Z_1; and, in general, Z_{i+1} extends from the beginning of Z^i to the end of the first occurrence of Y in Z^i, where Z^i is Z deprived of its initial segment $Z_1 Z_2 \cdots Z_i$. By construction, Y occurs in each Z_i terminally and only so; in view of §3, then, where the Z_i' are the results of putting X for Y in the respective Z_i,

$$(8)\qquad (i) \cdot sub1(Z_i', X, Y, Z_i).$$

Let '$Z_1 Z_2 \cdots Z_i$' and '$Z_1' Z_2' \cdots Z_i'$' be written '$Z_i!$' and '$Z_i'!$'. Thus

$$(9)\qquad Z_1! = Z_1 \cdot Z_1'! = Z_1',$$

$$(10)\qquad (i) \cdot Z_{i+1}! = Z_i! Z_{i+1} \cdot Z_{i+1}'! = Z_i'! Z_{i+1}',$$

and, by construction,

$$(11)\qquad (i) \cdot Z_i! \ init\ Z.$$

We exhaust the segments Z_i only when we reach a point in Z beyond which Y occurs no more. Thus, where Z_n is the last of the Z_i,

(12) $$(K)\colon Z = Z_n!K \cdot \supset \cdot Y \sim \textit{in } K.$$

Quantification with respect to subscripts, as in (8)–(11), refers of course only to the n or fewer significant values; for example, '$(i)\cdot\phi(Z_i, Z_i')$', '$(\exists i)\cdot\phi(Z_i, Z_i')$', and '$(i)\cdot\phi(Z_i, Z_{i+1})$' are short for

$$'\phi(Z_1, Z_1')\cdot\phi(Z_2, Z_2')\cdot \ldots \phi(Z_n, Z_n')',$$
$$'\phi(Z_1, Z_1')\vee\phi(Z_2, Z_2')\vee \ldots \phi(Z_n, Z_n')',$$

and

$$'\phi(Z_1, Z_2)\cdot\phi(Z_2, Z_3)\cdot \ldots \phi(Z_{n-1}, Z_n)'.$$

By §1, there are distinct atoms; let A and B be any two such, and, where k is the length of $Z_n'!Z_n!$, let $C = ABB\cdots B$ to k occurrences of B. Clearly

(13) $$(i)\cdot C \sim \textit{in } Z_i'!Z_i!,$$

since the length of C is greater by one even than that of $Z_n'!Z_n!$. Now it will be shown that, for any elements G and H such that $C \sim \textit{in } GH$, there are no occurrences of C in $CGCHC$ except the three indicated ones. First, no two occurrences of C can overlap; for, if they are distinct, one must start later than the other and hence must start at a non-initial place of the other; but all these non-initial places are occupied by B, whereas C starts with A. Hence if there is an occurrence of C in $CGCHC$ other than the three indicated ones, it overlaps none of the latter; it therefore lies wholly within G or H. But it cannot, since, by hypothesis, $C \sim \textit{in } GH$. Consequently there are none but the three occurrences of C in $CGCHC$. In particular, then, it follows from (13) that there are none but the three occurrences of C in $CZ_i'!CZ_i!C$.

Since, where

(14) $$D = CZ_1'!CZ_1!CCZ_2'!CZ_2!C\cdots CZ_n'!CZ_n!C,$$

D is made up wholly of segments of the form $CZ_i'!CZ_i!C$, any occurrence of C in D must lie either wholly within or partly within and partly beyond such a segment. But in the latter case the occurrence of C in question would overlap the terminal occurrence of C in $CZ_i'!CZ_i!C$, whereas we saw that no two occurrences of C could overlap. Hence every occurrence of C in D lies wholly within $CZ_i'!CZ_i!C$ for some i. But $CZ_i'!CZ_i!C$ was

seen to contain only the three indicated occurrences of C. Therefore D contains only the $3n$ occurrences of C indicated in (14).

Where $C \sim in\ GH$, $CGCHC$ contains, as was seen, only the three indicated occurrences of C, and is hence describable as beginning and ending with C and containing just three occurrences of C and no two adjacent. But, since D contains none but its $3n$ indicated occurrences of C, inspection of (14) shows that the only segments of D fulfilling this description of $CGCHC$ are the segments $CZ_i'!CZ_i!C$ for the various i; any other segment of D beginning and ending with C and containing three occurrences of C would contain two adjacent. Hence, if $C \sim in\ GH$ and $CGCHC\ in\ D$, $CGCHC$ must be $CZ_i'!CZ_i!C$ for some i; then G and H must be $Z_i'!$ and $Z_i!$. Thus, in view of D4,

$$(15)\quad (G)(H)\colon \Theta(G, H, C, D)\ .\supset.\ (\exists i)\cdot G = Z_i'!\ .\ H = Z_i!.$$

Conversely, by (14), (13), and D4,

$$(16)\qquad (i).\ \Theta(Z_i'!, Z_i!, C, D).$$

By (15) and (16),

$$(17)^*\quad (G)(H)\colon \Theta(G, H, C, D)\ .\equiv.\ (\exists i).\ G = Z_i'!\ .\ H = Z_i!.$$

If $sub1(U, X, Y, V)$, then, by §3, Y occurs in V terminally and only so and U is the result of putting X for Y in V. But, if V contains Y just thus and if further $Z_i!V\ init\ Z$, then V must be Z_{i+1}, so that U becomes Z_{i+1}'; and where U and V are Z_{i+1}' and Z_{i+1} it follows from (10) and (16) that $\Theta(Z_i'!U, Z_i!V, C, D)$. Thus

---

* This exemplifies a general technique, within a concatenation system, for eliminating reference to a finite class or relation of elements in favor of reference to two properly selected elements C and D. Where α is the m-adic relation (or class, if $m=1$) exhibited by just the elements $Q_{i1}, Q_{i2}, \cdots$, and Q_{im} in that order, for the various i from 1 to n, and k is the length of the element

$$Q_{11}Q_{12}\cdots Q_{1m}Q_{21}Q_{22}\cdots Q_{2m}\cdots Q_{n1}Q_{n2}\cdots Q_{nm},$$

and C is $ABB\cdots B$ to k occurrences of B, and D is

$$CQ_{11}CQ_{12}\cdots CQ_{1m}CCQ_{21}CQ_{22}\cdots CQ_{2m}C\cdots CQ_{n1}CQ_{n2}\cdots CQ_{nm}C,$$

it can be shown that

$$CG_1CG_2\cdots CG_mC \text{ in } D\cdot C \sim in\ G_1G_2\cdots G_m$$

if and only if $G_1, G_2, \cdots$, and G_m exhibit in that order the relation α. In (17) this equivalence is proved for the special case where $m=2$; G, H, $Z_i'!$, and $Z_i!$ answer to G_1, G_2, Q_{i1}, and Q_{i2}.

$(U)(V)(i)$: $sub1(U, X, Y, V) . Z_i! V \; init \; Z . \supset . \Theta(Z_i'! U, Z_i! V, C, D)$,

and hence

$(U)(V)$:. $sub1(U, X, Y, V) . \supset :$

$(S)(T)$: $(\exists i) . S = Z_i'! . T = Z_i! . TV \; init \; Z . \supset . \Theta(SU, TV, C, D)$;

that is, by (17),

(18) $(U)(V)$:. $sub1(U, X, Y, V) . \supset :$

$(S)(T)$: $\Theta(S, T, C, D) . TV \; init \; Z . \supset . \Theta(SU, TV, C, D)$.

Again, if Y occurs in V terminally and only so, and $V \; init \; Z$, then V must be Z_1; thus, where $sub1(U, X, Y, V)$ and $V \; init \; Z$, U and V will be Z_1' and Z_1. But, by (9) and (16), $\Theta(Z_1', Z_1, C, D)$. Thus

$(U)(V)$: $sub1(U, X, Y, V) . V \; init \; Z . \supset . \Theta(U, V, C, D)$.

From this and (18) it follows, by Dt1, that $\Phi(C, D)$. By Dt2, then,

$(G)(H)$:: $\Psi(W, G, H) . \supset :. \Theta(G, H, C, D) :.$

$W = G . Z = H . \vee : (\exists K) . Y \sim in \; K . W = GK . Z = HK$,

that is, by (17),

$(G)(H)$:: $\Psi(W, G, H) . \supset :. (\exists i) . G = Z_i'! . H = Z_i! :.$

$W = G . Z = H . \vee : (\exists K) . Y \sim in \; K . W = GK . Z = HK$,

and hence

$(\exists G)(\exists H) . \Psi(W, G, H) . \supset : (\exists i) : W = Z_i'! . Z = Z_i! . \vee :$

$(\exists K) . Y \sim in \; K . W = Z_i'! K . Z = Z_i! K$.

But, whether $Z = Z_i!$ or $(\exists K) . Y \sim in \; K . Z = Z_i! K$, i must be n: for in neither case does Z contain any occurrence of Y after $Z_i!$. Thus

(19) $(\exists G)(\exists H) . \Psi(W, G, H) . \supset . W = Z_n'! . Z = Z_n! . \vee :$

$(\exists K) . W = Z_n'! K . Z = Z_n! K$.

Of the occurrences of Y in Z, the one in Z_1 is, by construction, the first, the one in Z_2 is the first which begins after the end of that first, and so on. Therefore if each Z_i is supplanted in Z by

Z_i', so that $Z_n!$ is supplanted by $Z_n'!$, the result will be Z' as described in §2. Z' is thus $Z_n'!$ or $Z_n'!K$ according as Z is $Z_n!$ or $Z_n!K$. By (19), then,

$$(20) \qquad (\exists G)(\exists H).\ \Psi(W, G, H)\ .\supset .\ W = Z'.$$

If $\Phi(M, N)$, then, by Dt1,

$$sub1(Z_1', X, Y, Z_1)\ .\supset : Z_1\ init\ Z\ .\supset .\ \Theta(Z_1', Z_1, M, N)$$

and

$$(i):.\ sub1(Z_{i+1}', X, Y, Z_{i+1})\ .\supset : \Theta(Z_i'!, Z_i!, M, N)\ .$$
$$Z_i!Z_{i+1}\ init\ Z\ .\supset .\ \Theta(Z_i'!Z_{i+1}', Z_i!Z_{i+1}, M, N).$$

But these two results reduce, in view of (8)–(11), to

$$\Theta(Z_1'!, Z_1!, M, N)$$

and

$$(i): \Theta(Z_i'!, Z_i!, M, N)\ .\supset .\ \Theta(Z_{i+1}'!, Z_{i+1}!, M, N),$$

and from these it follows that $\Theta(Z_n'!, Z_n!, M, N)$. Thus

$$(21) \qquad (M)(N): \Phi(M, N)\ .\supset .\ \Theta(Z_n'!, Z_n!, M, N).$$

By (11) and D1, Z is $Z_n!$ or else $Z_n!K$ for some K; and, as seen above, Z' is in these respective cases $Z_n'!$ and $Z_n'!K$. Moreover, in view of (12), $Y \sim in\ K$. Thus

$$Z' = Z_n'!\ .\ Z = Z_n!\ .\vee : (\exists K).\ Y \sim in K\ .\ Z' = Z_n'!K\ .\ Z = Z_n!K.$$

From this and (21) it follows, by Dt2, that $\Psi(Z', Z_n'!, Z_n!)$. Hence

$$W = Z'\ .\supset .\ (\exists G)(\exists H).\ \Psi(W, G, H),$$

and consequently, by (20),

$$(\exists G)(\exists H).\ \Psi(W, G, H)\ .\equiv .\ W \simeq Z',$$

which was to be proved.

HARVARD UNIVERSITY

SOME PROPERTIES OF THE DISCRIMINANT MATRICES OF A LINEAR ASSOCIATIVE ALGEBRA*

BY R. F. RINEHART

1. *Introduction.* Let A be a linear associative algebra over an algebraic field. Let $e_1, e_2, \cdots, e_n$ be a basis for A and let c_{ijk}, $(i, j, k = 1, 2, \cdots, n)$, be the constants of multiplication corresponding to this basis. The first and second discriminant matrices of A, relative to this basis, are defined by

$$T_1(A) = \|t_1(e_re_s)\| = \left\| \sum_{i,j=1}^{n} c_{rsi}c_{ijj} \right\| = \left\| \sum_{i,j=1}^{n} c_{rij}c_{sji} \right\|,$$

$$T_2(A) = \|t_2(e_re_s)\| = \left\| \sum_{i,j=1}^{n} c_{rsi}c_{jij} \right\| = \left\| \sum_{i,j=1}^{n} c_{irj}c_{jsi} \right\|,$$

where $t_1(e_re_s)$ and $t_2(e_re_s)$ are the first and second traces, respectively, of e_re_s. The first forms in terms of the constants of multiplication arise from the isomorphism between the first and second matrices of the elements of A and the elements themselves. The second forms result from direct calculation of the traces of $R(e_r)R(e_s)$ and $S(e_r)S(e_s)$, $R(e_i)$ and $S(e_i)$ denoting, respectively, the first and second matrices of e_i. The last forms of the discriminant matrices show that each is symmetric.

E. Noether† and C. C. MacDuffee‡ discovered some of the interesting properties of these matrices, and shed new light on the particular case of the discriminant matrix of an algebraic equation. It is the purpose of this paper to develop additional properties of these matrices, and to interpret them in some familiar instances.

Let A be subjected to a transformation of basis, of matrix M,

$$e_i = \sum_{j=1}^{n} m_{ij}e_j, \qquad (i = 1, 2, \cdots, n; m = |m_{rs}| \neq 0).$$

---

* Presented to the Society, November 30, 1935. This paper, with proofs and details not included here, is on file as a doctoral thesis in the Library of the Ohio State University.

† Mathematische Zeitschrift, vol. 30 (1929), p. 689.

‡ Annals of Mathematics, (2), vol. 32 (1931), pp. 60–66; and Transactions of this Society, vol. 33 (1931), pp. 425–432.

MacDuffee noted* that under such a transformation the discriminant matrices are transformed by

$$T_1 = MT_1'M^T, \qquad T_2 = MT_2'M^T,$$

where M^T denotes the transpose of M; that is, these matrices are transformed in the same way as are the matrices of quadratic forms. Thence he proved that, if A has a principal unit, either discriminant matrix may be reduced to a diagonal form, $\|g_r\delta_{rs}\|$, by means of a transformation of basis which leaves the principal unit invariant. Further, for this normal basis the constants of multiplication satisfy the cyclic relations

$$g_p c_{rip} = g_i c_{pri}, \qquad (i, p, r = 1, 2, \cdots, n). \tag{1}$$

As a consequence of (1) he proved that for every choice of basis

$$S(x)T_i = T_iR(x), \qquad (i = 1, 2), \tag{2}$$

for every element x of A. In a subsequent paper L. E. Bush† extended MacDuffee's results to a general associative algebra.

2. *Another Reduction to Normal Form.* It is possible to derive the normal forms of the discriminant matrices of a general algebra by a method essentially simpler than that of Bush. Since no reduction is necessary if A is nilpotent, let A be non-nilpotent. Then A is the sum of a semi-simple component B and its radical N, which may be zero. Let $e_1, \cdots, e_p, e_{p+1}, \cdots, e_n$ be such a basis for A that $e_{p+1}, \cdots, e_n$ constitute a basis for N and $e_1, \cdots, e_p$ a basis for B, e_1 being the principal unit of B. Since both traces of a nilpotent element are zero, and since N is invariant in A,

$$T_i(A) = \begin{Vmatrix} t_i(e_1) & t_i(e_2) & \cdots & t_i(e_p) & 0 \cdots 0 \\ t_i(e_2) & t_i(e_2^2) & \cdots & t_i(e_2e_p) & 0 \cdots 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \cdots \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \cdots \cdot \\ t_i(e_p) & t_i(e_pe_2) & \cdots & t_i(e_p^2) & 0 \cdots 0 \\ 0 & 0 & \cdots & 0 & 0 \cdots 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \cdots \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \cdots \cdot \\ 0 & 0 & \cdots & 0 & 0 \cdots 0 \end{Vmatrix}, \tag{3}$$

* This property was earlier discovered by E. Noether, loc. cit.

† This Bulletin, vol. 38 (1932), pp. 49–51.

$(i=1, 2)$. Since e_1 is idempotent and F is non-modular, $t_i(e_1) \neq 0$, $(i=1, 2)$. Hence by a transformation of basis of A which leaves the basis of N unchanged and the principal unit of B invariant, $T_1(A)$ [or $T_2(A)$] can be reduced to a diagonal form $\|g_r\delta_{rs}\|$, where $g_i=0$, $(i>p)$. A manipulation of the associativity conditions for this normal basis yields (1) from which (2) may be derived.* From these relations we derive the following corollaries.

COROLLARY 1. *For every semi-simple algebra over the complex field, a basis can be so chosen that the first and second matrices of each element of the algebra are equal.*

COROLLARY 2. *If A is a commutative semi-simple algebra over the complex field, a basis for A can be so chosen that the first and second matrices of each element of A are equal and symmetric.*

For over the complex field a normal basis may be so chosen that $T(A)$ is scalar, whence (2) yields $S(x)=R(x)$. If A is also commutative, then $c_{ijk}=c_{jik}$ and

$$R^T(x) = S^T(x) = \sum_{i=1}^{n} x_i \|c_{rik}\|^T = \sum_{i=1}^{n} x_i \|c_{kir}\|$$

$$= \sum_{i=1}^{n} x_i \|c_{kir}\| = R(x) = S(x).$$

The existence of a normal basis can be applied to give a matric proof of the fact that a semi-simple algebra is the direct sum of simple algebras, and conversely. Let A be a semi-simple algebra with a proper invariant subalgebra B. Then if $e_1, \cdots, e_p, e_{p+1}, \cdots, e_n$ is a normal basis for A, and $e_1, \cdots, e_p$ the corresponding basis for B, the first and second matrices of the basal elements are

$$R(e_i) = \left\| \begin{matrix} R_B(e_i) & M_i \\ 0 & 0 \end{matrix} \right\|, \qquad S(e_i) = \left\| \begin{matrix} S_B(e_i) & 0 \\ M_i' & 0 \end{matrix} \right\|, \qquad (i \leqq p),$$

$$R(e_i) = \left\| \begin{matrix} P_i & Q_i \\ 0 & L_i \end{matrix} \right\|, \qquad S(e_i) = \left\| \begin{matrix} P_i' & 0 \\ Q_i' & L_i' \end{matrix} \right\|, \qquad (i > p),$$

where $R_B(e_i)$ and $S_B(e_i)$ denote, respectively, the first and sec-

* It should be noted that the restriction on the field F is necessary only for the reduction to normal form; by direct verification it is easily seen that (2) holds for any basis, *regardless of the nature of F.*

ond matrices of e_i, the representation being based on the algebra B only. Further, for this basis,

$$T_1(A) = \left\| \begin{matrix} T_1(B) & 0 \\ 0 & W \end{matrix} \right\|,$$

where $T_1(B)$ and W are non-singular. Hence, applying (2),

$$M_i = M_i' = 0, \quad (i \leqq p); \qquad Q_i = Q_i' = 0, \quad (i > p).$$

By means of the cyclic relations we find further that $P_i = P_i' = 0$, $(i > p)$. Hence

$$R(x) = \left\| \begin{matrix} R_B(x) & 0 \\ 0 & R_C(x) \end{matrix} \right\|, \qquad S(x) = \left\| \begin{matrix} S_B(x) & 0 \\ 0 & S_C(x) \end{matrix} \right\|.$$

Obviously the system of matrices $R_e(x)$ $[S_e(x)]$ is closed under addition and multiplication, and the L_i $[L_i']$ are linearly independent. Hence the linear system $(e_{p+1}, \cdots, e_n)$ is an algebra,* and therefore $A = B + C$,† where B and C are semi-simple algebras. This process can be continued with B and C in place of A, and so on, until A is decomposed into simple components. That the decomposition is unique may be proved as in Dickson's *Algebren und ihre Zahlentheorie.*

The converse of this theorem is immediate from the standpoint of the discriminant matrix. For the first discriminant matrix of a direct sum of algebras is the direct sum of the first discriminant matrices of the component algebras,‡ whence, if each component is simple, and non-null, each of the component matrices is non-singular, and therefore so is the direct sum.

3. *Equality of T_1 and T_2.* Since T_1 and T_2 are transformed cogrediently, their equality is an invariant property of A. If A is nilpotent, then $T_1(A) = T_2(A) = 0$. Suppose then that A is non-nilpotent, with the basis $e_1, \cdots, e_p, \cdots, e_n$, where $e_{p+1}, \cdots, e_n$ constitute a basis for the radical (if any), and $e_1, \cdots, e_p$ a basis for the semi-simple component of A. For this

* Since A is semi-simple, it is equivalent to the algebra of its first [second] matrices.

† $+$ denotes direct sum.

‡ MacDuffee, Annals of Mathematics, loc. cit.

basis T_1 and T_2 are in the form (2). Hence an obvious necessary condition that $T_1 = T_2$ is

$$t_1(e_r) = t_2(e_r), \qquad (r = 1, 2, \cdots, p). \tag{4}$$

This condition is clearly sufficient, since (4) implies

$$t_1(e_r e_s) = \sum_{i=1}^{p} c_{rsi} t_1(e_i) = \sum_{i=1}^{p} c_{rsi} t_2(e_i) = t_2(e_r e_s).$$

Now (4) implies that $t_1(x) = t_2(x)$ for every x of A, and conversely. Hence if x is any element of A, and if $T_1 = T_2$, then $t_1(x^i) = t_2(x^i)$ for every i. By a theorem of Frobenius* this implies that

$$s_i = s_i', \qquad (i = 1, 2, \cdots, n),$$

s_i and s_i' being the sum of the ith powers of the first and second characteristic roots, respectively, of x. By Newton's identities this implies that the first and second characteristic functions of x are equal. Conversely, if the characteristic functions of each element x are equal, then so are the two traces of x.

THEOREM 1. *The discriminant matrices are equal if, and only if, the characteristic functions of each element of the algebra are equal.*

If A is semi-simple, then $T_1(A)$ is non-singular and (2) may be written $S(x) = T_1 R(x) T_1^{-1}$; hence, $S(x)$ and $R(x)$ being similar, the characteristic functions are equal. This proves the following corollary.

COROLLARY. *If A is semi-simple, $T_1(A) = T_2(A)$.*†

By a further elementary analysis, which is omitted here, it may be shown that: *The equality of $T_1(A)$ and $T_2(A)$, when A is neither semi-simple nor nilpotent, depends only on the multiplicative relations existing between the radical of A and any semi-simple component B of A. In particular, if N is commutative with B, then $T_1(A)$ is equal to $T_2(A)$.*

C. C. MacDuffee‡ defined $\rho(\sigma)$ to be the maximum number of linearly independent linear relations among the first matrices $R(e_i)$ $[S(e_i)]$ of an algebra. and proved that ρ is equal to the

* G. Frobenius, Journal für Mathematik, vol. 51 (1856), pp. 209–271.

† Proved by MacDuffee by manipulation of the cyclic relations.

‡ This Bulletin, vol. 35 (1929), pp. 344–349.

order of the maximal zero subalgebra Z, such that $ZA=0$, and σ is equal to the order of a similar algebra W, such that $AW=0$. By a long but elementary analysis omitted here, the following theorem can be proved.

THEOREM 2. *If A is a non-nilpotent algebra with a commutative radical N, a necessary and sufficient condition that $\rho=\sigma$ is that $t_1(u)=t_2(u)$, where u is any principal idempotent of A.*

COROLLARY. *If A is non-nilpotent and has a commutative radical, and if $T_1(A)=T_2(A)$, then $\rho=\sigma$.*

It can be shown by examples that the condition $t_1(u)=t_2(u)$ is in general neither necessary nor sufficient, if N is not commutative.

4. *The Discriminant Matrix of an Algebraic Equation.* We shall now consider two applications of the foregoing theory to the case of the commutative algebra generated by an algebraic equation. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \tag{5}$$

be an equation with coefficients in a field F. Let A be the ring consisting of all polynomials with coefficients in F, reduced modulo $f(x)$, or, what is the same thing, the algebra generated by an element x, whose minimum equation is (5). For the customary basis $1, x, x^2, \cdots, x^{n-1}$, the discriminant matrix of A is*

$$T(A) = \begin{Vmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{Vmatrix},$$

where s_i is the sum of the ith powers of the roots of (5), s_0 being defined to be n.

If we form the equality (2) and equate corresponding elements of the resulting matrices, discarding the immediate identities, we obtain

$$-\sum_{i=0}^{n-1} a_i s_{i+j} = s_{n+j}, \qquad (j = 0, 1, \cdots, n-2),$$

* MacDuffee, Annals of Mathematics, loc. cit.

which are Newton's identities for s_k, $(k=n, n+1, \cdots, 2n-2)$. Again, if we form $S(x^2)T=TR(x^2)$, we get the additional identity for s_{2n-1}. Similarly, if (2) is applied with $x^3, x^4, \cdots$, all the Newtonian identities for s_k, $(k \geqq n)$ are obtained. Conversely, Newton's identities for $k \geqq n$ imply that $S(x)T=TR(x)$. Thus (2) may be considered as an extension of Newton's identities to a general algebra.

The second application has to do with the following theorem.

BORCHARDT-JACOBI THEOREM. *If $f(x)=0$ is an algebraic equation with real coefficients, the number of its distinct roots is equal to the rank of the discriminant matrix, and the number of its distinct real roots is equal to the signature of this matrix.**

We shall outline a proof of the first half of this theorem, using the discriminant matrix from the standpoint of linear algebra. Let

$$f(x) = \prod_{i=1}^{m} (x - \alpha_i)^{n_i} = 0 \tag{6}$$

be an algebraic equation with the distinct roots $\alpha_1, \cdots, \alpha_m$. Let $m<n$ and let A be the algebra defined by $f(x)=0$.† If we define $P(x)=\prod_{i=1}^{m}(x-\alpha_i)$, the elements of the set of polynomials

$$P(x), xP(x), \cdots, x^{n-m-1}P(x), \tag{7}$$

are linearly independent and each one (hence any linear combination of them) is nilpotent. It is easily seen that any nilpotent polynomial must contain the factor $P(x)$, and consequently the set (7) is a maximal such set and therefore constitutes a basis for the radical of A. Hence the discriminant matrix of A is of nullity $n-m$, that is, of rank m. If $m=n$, it can be shown that there are no nilpotent elements, and hence no radical in A, whence the rank of the discriminant matrix is n.

ASHLAND COLLEGE,
ASHLAND, OHIO

* A. Loewy, Ostwald's Klassiker der exakten Wissenschaften, No. 143, pp. 50–63.

† The ground field F is here taken to be the complex field. The same proof, with only slight modifications, can be carried through if F is considered to be any subfield of the complex field.

DERIVED SETS AND THEIR COMPLEMENTS

BY S. T. SANDERS, JR.

1. *Introduction.* Denoting by gA the derived set of a set A in a general topological space* S, and by cA the complement $S-A$ of A, we consider the family of sets ϕA, where ϕ is a product involving the operator c and operators of the form g^α, α being an ordinal, finite or transfinite. Important examples of operators are cg, gc, g^2c, cgc. The following discussion is based on the assumption of the distributive and closure properties:

I. $$g(A+B) = gA + gB,$$

II. $$g^2A \subset gA.$$

In §§2–5 eight *elementary* sets are defined, from which a *canonical* system of sets is obtained. This canonical system is sufficient for the representation of all sets of the form ϕA and the finite sums and products $\Sigma\phi A$, $\Pi\phi A$, and $\Sigma\Pi\phi A$, with the exception of certain subsets of the derived set of the isolated points of the space S. In §6 specializations of the general theory are given to spaces possessing either or both of the properties: (a) self density, (b) $g0=0$. Under restrictions (a) and (b), the basic set of inclusions (10), which is fundamental for the discussion of §§4 and 5, is found to be logically equivalent to a set of inclusions given by Kuratowski† for the set $\overline{A}$, having the properties of the closure $A+gA$ of A. In §7 are presented various properties of the elementary sets. All relations are established formally, though Axioms I, II are equivalent to the assumption of a neighborhood space with open sets for neighborhoods, so that all results may be had by classification of neighborhoods with respect to the distribution of the points of A and cA. The symbols $\rightarrow$ and $\subset$ denote respectively implication and inclusion.

* See M. Fréchet, *Les Espaces Abstraits*, 1928; E. W. Chittenden, *On general topology*, Transactions of this Society, vol. 31 (1929), pp. 290–321; W. Sierpinski, *La notion de dérivée comme base d'une théorie des ensembles abstraits*, Mathematische Annalen, vol. 97 (1926), pp. 321–337.

† C. Kuratowski, *Sur l'opération $\overline{A}$ de l'analysis situs*, Fundamenta Mathematica, vol. 3 (1922), pp. 182–199.

2. *Reduction Formulas.* From the distributive law I we have $gA + gcA = gS$. Taking complements, we obtain the following lemma.

LEMMA 1. *We have* $cgA \subset gcA + J$, *where* $J = cgS$, *the set of isolated points of the space.*

From I also follows the monotonic property

$$X \subset Y \rightarrow gX \subset gY. \tag{1}$$

Since $X \subset Y \rightarrow cY \subset cX$, we have also, by (1),

$$\begin{aligned} X \subset Y &\rightarrow gcY \subset gcX, \\ &\rightarrow cgY \subset cgX, \\ &\rightarrow gcgY \subset gcgX. \end{aligned}$$

Instead of referring to the monotonic property (1), it will be frequently convenient to speak of *operating with* g *on* $X \subset Y$. Likewise we shall operate with c, $gc, \cdots$.

LEMMA 2. *For any operator* ϕ, $J \subset cg\phi A$.

The lemma follows on applying the operator cg to the inclusion $\phi A \subset S$.

LEMMA 3. *For any operator* ϕ, $gJ \subset gcg\phi A$.

This is an immediate consequence of (1) and Lemma 2.

The following reduction formulas hold for any ordinal α.

FORMULA I. $gcgA = gcg^{\alpha}A$. Operating with g on Lemma 1, we obtain by the closure property II,

$$gcgA \subset g^2cA + gJ \subset gcA + gJ, \tag{2}$$

whence, on replacing A by gA, we find $gcg^2A \subset gcgA + gJ$; or by Lemma 3, $gcg^2A \subset gcgA$. The reversed inclusion is obtained by operating with gc on the inclusion $g^2A \subset gA$, so that we shall have $gcgA = gcg^2A$. Replacing A by gA, we get $gcgA = gcg^3A$, and the desired relation follows at once.

FORMULA II. $gcgA = g^{\alpha}cgA + gJ$. Replacing A by cgA in $g^2A \subset gA$, we shall have $g^2cgA \subset gcgA$, whence, by Lemma 3,

$$g^2cgA + gJ \subset gcgA. \tag{3}$$

Replacing A by gA in (2), we get $gcg^2A \subset g^2cgA + gJ$, whence, by Formula I, $gcgA \subset g^2cgA + gJ$. From this and (3) follows

$$gcgA = g^2cgA + gJ. \tag{4}$$

Operating on (4) with g, we have $g^2cgA = g^3cgA + g^2J$, whence (4) may be written in the form $gcgA = g^3cgA + gJ$. The required formula follows immediately.

Preliminary to Formula III we have the following lemma.

LEMMA 4. $gXcgcY \subset g(XY) \subset gXgY$.

The second inclusion is a direct consequence of the monotonic property. As for the first, we may write, by I,

$$gX = g(XY + XcY) = g(XY) + g(XcY),$$

whence

$$gXcgcY = [g(XY) + g(XcY)]cgcY \subset g(XY) + g(XcY)cgcY; \tag{5}$$

but, by the second inclusion of the lemma, $g(XcY) \subset gXgcY$, so that we have $g(XcY)cgcY \subset gXgcYcgcY = 0$, and, by (5), the lemma is established.

FORMULA III. $gcgA = gcgcgcgA$. In Lemma 1 we replace A by cgA, obtaining, by II, $cgcgA \subset g^2A + J \subset gA + J$, whence, on operating by g,

$$gcgcgA \subset g^2A + gJ \subset gA + gJ. \tag{6}$$

Again, replacing A by cgA, we have, by Lemma 3,

$$gcgcgcgA \subset gcgA + gJ = gcgA.$$

To establish the reversed inclusion, we proceed as follows. Operating on (6) with gc, we have

$$g(cgAcgJ) \subset gcgcgcgA. \tag{7}$$

Now in Lemma 4, on setting $X = cgA$, $Y = cgJ$, we shall have $gcgAcg^2J \subset g(cgAcgJ)$, or by the closure property,

$$gcgA \subset g(cgAcgJ) + gJ. \tag{8}$$

But, by Lemma 3, $gJ \subset g(cgAcgJ)$, so that (8) reduces to

$$gcgA \subset g(cgAcgJ). \tag{9}$$

By (7) and (9) the desired relation is established.

3. *A Canonical System of Sets.* Consider now a set ϕA, where ϕ is any combination of the deriving and complementing operations. By Formulas I, III, we have

$$g^{\alpha}cg^{\beta}cg^{\gamma}cg^{\delta}A = g^{\alpha}cgcgcgA = g^{\alpha}cgA.$$

Thus it appears that when any derived set of A is operated on with gc, the only distinct sets obtainable by further operations with g and c are of the types $g^{\alpha}cgA$, $cg^{\alpha}cgA$, $g^{\alpha}cgcgA$, $cg^{\alpha}cgcgA$. The following theorem is thus established.

THEOREM 1. *For any operator ϕ, the set ϕA reduces to A, cA, cgA, $cgcA$, $cgcgA$, $cgcgcA$, or else may be obtained by operating on one of these sets with g^{α} or cg^{α}.*

4. *Definition of the Elementary Sets.* The following lemma is needed.

LEMMA 5. *For any ordinals α, β, and operator ϕ,*

$$g^{\alpha}cg\phi A = g^{\beta}cg\phi AcgJ + g^{\alpha}cg\phi AgJ,$$

$$cg^{\alpha}cg\phi A = cg^{\beta}cg\phi AcgJ + cg^{\alpha}cg\phi AgJ.$$

By the closure property and the Formula II previously stated, we have

$$g^{\alpha}cg\phi A \subset gcg\phi A = g^{\beta}cg\phi A + gJ,$$

whence we obtain $g^{\alpha}cg\phi AcgJ = g^{\beta}cg\phi AcgJ$, and

$$g^{\alpha}cg\phi A = g^{\alpha}cg\phi AcgJ + g^{\alpha}cg\phi AgJ = g^{\beta}cg\phi AcgJ + g^{\alpha}cg\phi AgJ.$$

The rest of the lemma follows on taking complements.

The following fundamental inclusions hold for all values of α.

I1. $$cg^{\alpha}cAc\bar{J} \subset cgcgcgcAcJ.$$

Operating on (6) with $cg^{\alpha-1}$, and replacing A by cA, we have $cg^{\alpha}cAcgJ \subset cg^{\alpha}cgcgcA$, whence $cg^{\alpha}cAcgJ \subset cg^{\alpha}cgcgcAcgJ$. But, choosing $\beta = 1$ in Lemma 5, we have $cg^{\alpha}cgcgcAcgJ = cgcgcgcAcgJ$, so that the preceding inclusion becomes, by Lemma 3,

$$cg^{\alpha}cAcgJ \subset cgcgcgcAcgJ = cgcgcgcA.$$

Multiplying by cJ, we have $cg^{\alpha}cAc\bar{J} = cg^{\alpha}cAcgJ \subset cgcgcgcAcJ$, which is the desired inclusion.

I2. $$cgcgcgcAcJ \subset g^{\alpha}cgcA.$$

In Lemma 1 we replace A by $cgcgcA$, and have, by II,

$$cgcgcgcA \subset g^2cgcA + J \subset gcgcA + J.$$

Multiplying by $cgJcJ$, we obtain $cgcgcgcAcJ \subset gcgcAcgJcJ$, by Lemma 3. But by Formula II, $gcgcAcgJ = g^acgcAcgJ$, whence the above inclusion yields $cgcgcgcAcJ \subset g^acgcAcgJcJ \subset g^acgcA$.

I3. $$cgcgcgcAcJ \subset cg^acgA.$$

Applying the operator gc to (2), we get $g(cgcAcgJ) \subset gcgcgA$. Since, by (9), $gcgcA \subset g(cgcAcgJ)$, we have then $gcgcA \subset gcgcgA$, or, replacing A by cA, $gcgA \subset gcgcgcA \subset gcgcgcA + J$. From the closure of derived sets, we have $g^acgA \subset gcgA \subset gcgcgcA + J$. On taking complements, the desired inclusion is obtained.

By operating with c on I3, I2, I1, respectively, and replacing A by cA, the following inclusions are obtained:

I4. $$g^acgcA \subset gcgcgA + J.$$

I5. $$cg^acgA \subset gcgcgA + J.$$

I6. $$gcgcgA + J \subset g^aA + \bar{J}.$$

Consider now the following special forms of the inclusions I1–I6, where α_1 and α_2 are the least ordinals α such that g^acgcA and g^acgA, respectively, are perfect:

$$(10)\quad cgcAc\bar{J} \subset cgcgcgcAcJ \begin{matrix} \subset g^{\alpha_1}cgcA \subset \\ \subset cg^{\alpha_2}cgA \subset \end{matrix} gcgcgA + J \subset gA + \bar{J}.$$

From the monotonic nature of the six sets (10), it is seen that the first, the complement of the sixth, and the differences of the sixth and fifth, the fifth and second, and the second and first, are mutually disjoined and fill the space S. The difference of the fifth and second sets, namely, $(gcgcgA+J)\ (gcgcgcA+J)$, may be decomposed into four non-overlapping sets by means of the intervening sets, $g^{\alpha_1}cgcA$ and $cg^{\alpha_2}cgA$. Thus we obtain a decomposition of S into eight non-overlapping sets. With certain reductions by (10), Lemmas 2 and 3, we list these eight sets, and shall refer to them as elementary or, more briefly, E sets:

$$\begin{aligned}
&E_1 = cgcAc\bar{J}, \qquad E_2 = cgcgcgcAcJc(cgcAc\bar{J}) = cgcgcgcAgcA,\\
&E_3 = g^{\alpha_1}cgcAcg^{\alpha_2}cgAc(cgcgcgcAcJ) = g^{\alpha_1}cgcAcg^{\alpha_2}cgAgcgcgcA,\\
&E_4 = cgAc\bar{J}, \qquad E_5 = (gA + \bar{J})c(gcgcgA + J) = gAcgcgcgA,\\
&E_6 = (gcgcgA + J)cg^{\alpha_1}cgcAc(cg^{\alpha_2}cgA) = gcgcgAcg^{\alpha_1}cgcAg^{\alpha_2}cgA\\
&E_7 = g^{\alpha_1}cgcAg^{\alpha_2}cgA, \qquad E_8 = cg^{\alpha_1}cgcAcg^{\alpha_2}cgA.
\end{aligned} \tag{11}$$

It is seen that the replacement of A by cA interchanges E_1 and E_4, E_2 and E_5, E_3 and E_6. Thus, corresponding to a theorem holding for a set of one of these pairs, there is an identical theorem valid for the other set. We shall make use of this symmetry.

5. *The General Canonical System.*

LEMMA 6. $J \subset E_8$; $gJ \subset E_3+E_6+E_7+E_8$.

It is seen by (11) that every E set except E_8 has either the factor cJ or else a factor $g\phi A$, and so by Lemma 2 is disjoined from J. Likewise E_1 and E_4 contain the explicit factor cgJ, while E_2 and E_5 have factors $cgcgcgcA$ and $cgcgcgA$, which by Lemma 3 are contained in cgJ.

By Lemma 6, 3, and 5, we may obtain from (11) the following decomposition of the sets mentioned in Theorem 1.

$$
\begin{aligned}
g^acgA &= E_4+E_5+cgJ(E_6+E_7)+g^acgAgJ.\\
cg^acgA &= E_1+E_2+cgJ(E_3+E_8)+cg^acgAgJ.\\
g^acgcA &= E_1+E_2+cgJ(E_3+E_7)+g^acgcAgJ.\\
cg^acgcA &= E_4+E_5+cgJ(E_6+E_8)+cg^acgcAgJ.\\
g^acgcgA &= E_1+E_2+cgJ(E_3+E_6+E_7)+c\bar{J}E_8+g^acgcgAgJ.\\
cg^acgcgA &= E_4+E_5+J+cg^acgcgAgJ.\\
g^acgcgcA &= E_4+E_5+cgJ(E_3+E_6+E_7)+c\bar{J}E_8+g^acgcgcAgJ.\\
cg^acgcgcA &= E_1+E_2+J+cg^acgcgcAgJ.
\end{aligned}
\tag{12}
$$

Expressions for the sets g^aA, cg^aA, g^acA, cg^acA of Theorem 1 in terms of the E sets cannot be obtained in this manner, since Lemma 5 does not apply to these sets. We have instead the following lemma.

LEMMA 7.

$$P_1cgJ = E_1 + E_2 + cgJ(E_3 + E_6 + E_7) + c\bar{J}E_8 + P_1E_5,$$

$$P_2cgJ = P_2E_2 + cgJE_3 + E_4 + E_5 + cgJ(E_6 + E_7) + c\bar{J}E_8,$$

where P_1, P_2, are respectively the perfect components of A, cA.

By (11), Lemma 6, and I6, we have for every α

$$E_1 + E_2 + cgJ(E_3 + E_6 + E_7) + c\bar{J}E_8 = gcgcgAc\bar{J} \subset g^aA. \tag{13}$$

Since E_4 is disjoined from gA, the lemma follows.

By (11) and Lemma 7 we have

$$
\begin{aligned}
g^\alpha A &= E_1 + E_2 + cgJE_3 + P_1E_5 + \textstyle\sum_{\beta \geqq \alpha} (g^\beta A - g^{\beta+1}A) \\
&\quad + cgJ(E_6 + E_7) + c\bar{J}E_8 + P_1gJ, \\
cg^\alpha A &= E_4 + \textstyle\sum_{\beta < \alpha} (g^\beta A - g^{\beta+1}A) + J + gJcg^\alpha A, \\
g^\alpha cA &= P_2E_2 + \textstyle\sum_{\beta \geqq \alpha} (g^\beta cA - g^{\beta+1}cA) + cgJE_3 + E_4 + E_5 \\
&\quad + cgJ(E_6 + E_7) + c\bar{J}E_8 + P_2gJ, \\
cg^\alpha cA &= E_1 + \textstyle\sum_{\beta < \alpha} (g^\beta cA - g^{\beta+1}cA) + J + gJcg^\alpha cA.
\end{aligned} \tag{14}
$$

In (12) and (14) we have the required decomposition of the sets of Theorem 1. Since by (13) each set $g^\beta A - g^{\beta+1} A$ lies in $E_5 + gJ$, we may sum up our results in the following theorem.

THEOREM 2. *Any finite sum of finite products $\Sigma\Pi\phi A$ is expressible, aside from a subset of gJ, as a sum chosen from E_1, P_2E_2, $g^\beta cA - g^{\beta+1}cA$, $cgJE_3$, E_4, P_1E_5, $g^\beta A - g^{\beta+1}A$, $cgJE_6$, $cgJE_7$, $c\bar{J}E_8$, J, and products of these sets by A and cA.*

To illustrate, consider the set $X = g^2cgcgcgAcgcg^2cgAg^3AgcgA$. Applying Formulas I and III, we have $X = g^2cgAcgcgcgAg^3AgcgA$, whence by the closure of derived sets, $X = g^2cgAcgcgcgAg^3A$. Finally, (12) and (14) give $X = P_1E_5 + \sum_{\beta \geqq 3}(g^\beta A - g^{\beta+1}A)$, aside from a subset of gJ.

6. *Specializations.* Most of the spaces commonly occurring in geometry and analysis, such as Euclidean n-space, Hilbert space, and all continua, have the self-dense property, and also the property $g0 = 0$. If we set $J = gJ = 0$, the results of the preceding sections are considerably simplified. Formula II reduces to $gcgA = g^\alpha cgA$, and the inclusions (10) become*

$$
cgcA \subset cgcgcgcA \begin{matrix} \subset gcgcA \subset \\ \subset cgcgA \subset \end{matrix} gcgcgA \subset gA. \tag{15}
$$

The elementary sets (11) reduce to

$$
\begin{aligned}
&E_1 = cgcA, \quad E_2 = cgcgcgcAgcA, \quad E_3 = gcgcgcAgcgcAcgcgA, \\
&E_4 = cgA, \quad E_5 = gAcgcgcgA, \quad E_6 = gcgcgAgcgAcgcgcA, \\
&E_7 = gcgcAgcgA, \quad E_8 = cgcgcAcgcgA,
\end{aligned} \tag{16}
$$

* These inclusions are given by Kuratowski, loc. cit., for the closure function.

while the general canonical system of §5 reduces to

$$(17)\qquad E_1,\quad P_2E_2,\quad \sum(g^\delta cA - g^{\delta+1}cA),\quad E_3,\quad E_4,\quad P_1E_5,\quad \sum(g^\delta A - g^{\delta+1}A),\quad E_6,\quad E_7,\quad E_8.$$

The requirement $gJ=0$ yields a space slightly more general than the preceding, including the case where isolated points J exist, yet have a null derived set. The formulas of §§2–5 specialize, however, to the very forms (15), (16), (17). The structure of the E sets is unchanged except that E_8 includes the set J.

We may also specialize the formulas of §§2–5 by requiring $J=0$, thus including the case $J=gJ=0$ and also the case where the derived set of the null set is not null. By the monotonic property we have for every set A, $g0=gJ\subset gA$, so that the inclusions (10) again reduce to (15), and the definitions (16) hold without change. Since $gJ\subset gA$, we see that E_7 includes gJ.

If we require $J+gJ=S$, the canonical system of Theorem 2 is considerably simplified, since the inclusions (10) reduce to

$$0 \begin{matrix} \subset g^{\alpha_1}cgcA \subset \\ \subset cg^{\alpha_2}cgA \subset \end{matrix} S,$$

so that the only non-null E sets are E_3, E_6, E_7, E_8.

7. *The Nature of the Elementary Sets.* The following theorems may be obtained.

THEOREM 3. *$E_1+E_4+E_8+gJ$ is dense on gS.*

THEOREM 4. $E_3cgJ=gE_1cgE_4gE_8cgJ$.

THEOREM 5. $E_2=cgJgE_1cgE_4cgE_8gcA$.

THEOREM 6. $gE_3\subset E_3+E_7$.

THEOREM 7. $gE_2\subset E_2+E_3+E_7+gJ$.

THEOREM 8. $gE_8\subset E_3+E_6+E_7+E_8$.

In a space $J=gJ=0$ it is evident that $E_8=cgE_1cgE_4$, and $E_7=gE_1gE_4$. If the space is also of n dimensions, then it follows from Theorem 3 that E_1, E_4, and E_8 are n-dimensional or else null, whereas the remaining E sets are at most $(n-1)$-dimensional. Specializing further, we have the following result.

THEOREM 9. *In a Euclidean space of more than one dimension, $E_7\subset gE_7+gE_3gE_6$.*

ST. JOSEPH, MISSOURI

THE VENERONI TRANSFORMATION IN S_n*

BY VIRGIL SNYDER AND EVELYN CARROLL-RUSK

1. *Introduction.* The purpose of the present paper is to obtain the system of bilinear equations of the Veneroni transformation defined by associating projectively the primes (or hyperplanes) of S_n with the primals (or hypersurfaces) V^n of order n through $n+1$ arbitrary S'_{n-2} of S'_n, and to derive a complete scheme of mapping of the manifolds of either space on the linear manifolds of the other. Both of these are believed to be new.

2. *Analytic Expression for the Veneroni Transformation.* The process is somewhat different according as n is odd or even. It will be most easily understood by considering in detail the case $n=5$. In S_5 six three way spaces σ_i, $(i=1, 2, \cdots, 6)$, form the base of a Veneroni transformation. Let $\sigma_1 \equiv x_1=0$, $x_2=0$; $\sigma_2 \equiv x_3=0, x_4=0$, $\sigma_3 \equiv x_5=0, x_6=0$, and $\sigma_4 \equiv a=\sum_{i=1}^{6} a_i x_i=0$, $b=0$; $\sigma_5 \equiv c=0$, $d=0$; $\sigma_6 \equiv e=0$, $f=0$. Through five of the σ_i (not σ_k) passes one and only one V_4^4, say V_k, determined by the ∞^2 lines meeting all of them. This and any S_4 of the pencil through the remaining σ_k provides one composite quintic primal of the system. Thus a complete homaloidal system is obtained. Among these primals six independent identities exist of the form

$$x_2 V_1 = (e_1 f)V_6 + (c_1 d)V_5 + (a_1 b)V_4,$$

in which $(a_i b)=a_i b(x)-b_i a(x), \cdots$. If $\rho x'_1 = x_1 V_1$, $\rho x'_2 = x_2 V_1$, $\rho x'_3 = x_3 V_2, \cdots$, we may write

$$\frac{a(x)}{b(x)} = -\frac{\sum B_i x'_i}{\sum A_i x'_i},$$

and so on where B_i is the cofactor of b_i in the determinant

$$D = |a_1 b_2 c_3 d_4 e_5 f_6|,$$

after the transpositions (12), (34), (56) have been made in the subscripts. Any two of these and the three equations

$$x_1 x'_2 - x'_1 x_2 = 0, x_3 x'_4 - x'_3 x_4 = 0, x_5 x'_6 - x'_5 x_6 = 0$$

---

* Presented to the Society, September 11, 1935.

completely define the transformation. A similar statement holds for n any odd number. For n, even a slight variation in the procedure must be introduced, since the equations of the σ_i can not all be taken as part of the simplex of reference.

3. *Double Elements of V_{n-1}^{n-1} in S_n.* Any two primals of S_{n-1} of the system, V_α and V_β, have in common all the $[n-2]$-dimensional bases σ_i except σ_α and σ_β; a ruled manifold $R_{n-2}^{(n+1)(n-2)/2}$ of order $(n+1)(n-2)/2$ consisting of the lines intersecting all the σ_i; and a residual manifold $M_{n-2}^{(n-2)(n-3)/2}$ of order $(n-2)(n-3)/2$.

The bases σ_i, σ_k meet in an $[n-4]$-space denoted by σ_{ik}. The spaces $\sigma_{12}, \sigma_{13}, \cdots, \sigma_{1(n+1)}$ are double and lie in σ_1. On an $[n-1]$-primal, such as V_{n+1}, the bases $\sigma_{12}, \sigma_{13}, \cdots, \sigma_{1n}$ lie in an S_{n-2} and are intersected by a ruled manifold $R_{n-4}^{(n-1)(n-4)/2}$. These $[n-4]$-spaces $\sigma_{12}, \sigma_{13}, \cdots, \sigma_{1n}$ and the generators of the ruled manifold are double on V_{n+1} and form the base of a homaloidal system of primals in S_{n-1} in σ_1. The manifolds of this system which are cut by V_α and V_β intersect therefore in a normal variety M_{n-2} of S_{n-2}, which is a double manifold intersecting each base σ_{ik} in $n-3$ points and not intersecting any generator of $R_{n-4}^{(n-1)(n-4)/2}$. In the general case, there are no other double elements. Similarly, the presence of triple and other multiple loci on each V_{n-1}^{n-1} of the system can be obtained.

For $n=5$, on each V_4^4 containing five base three spaces σ_i there are twenty double lines and five double space cubic curves, all lying in the base spaces σ_i. These results were obtained by Eiesland* by the method of differential geometry.

4. *Residual Intersection of Two V_{n-1}^{n-1} in S_n.* The intersection of V_α and V_β, which is of order $(n-1)^2$, consists of $n-1$ of the bases σ_i, of the ruled manifold $R_{n-2}^{(n+1)(n-2)/2}$, and of a residual manifold of order $(n-2)(n-3)/2$.

Each S_{n-1} of the pencil $|\sigma_k|$, $(k \neq \alpha, \beta)$, meets each of the $n-1$ remaining σ_i, $(i \neq \alpha, \beta)$, in an S_{n-3}. These S_{n-3} intersect in pairs in $[n-5]$-spaces S_{n-5}, belonging to a common $[n-3]$-space K_{n-3} which meets each S_{n-3} in an S_{n-4}. This K_{n-3} is also incident to the σ_k and meets σ_α and σ_β. Hence it lies on V_α and V_β and, consequently, on each primal of the pencil. As S_{n-1} describes the pencil $|\sigma_k|$, this K_{n-3} describes the variety $M_{n-2}^{(n-2)(n-3)/2}$. Its equations are

* J. Eiesland, Palermo Rendiconti, vol. 54 (1930), pp. 335–365.

$$\frac{x_1}{x_2} = \frac{(a_3b_2)x_3 + (a_4b_2)x_4}{(a_1b_3)x_3 - (a_4b_1)x_4} = \frac{(a_5b_2)x_5 + (a_6b_2)x_6}{(a_1b_5)x_5 - (a_6b_1)x_6} = \cdots$$
$$= \frac{(a_nb_2)x_n + (a_{n+1}b_2)x_{n+1}}{(a_1b_n)x_n - (a_{n+1}b_1)x_{n+1}}.$$

For $n=5$, if V_5 and V_6 are determined by $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_6$ and $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$, respectively, the intersection consists of the bases $\sigma_1, \sigma_2, \sigma_3, \sigma_4$, of the three-dimensional variety $R_3{}^9$, and of a residual variety of order three. Each of the S_4 of the pencil $|\sigma_4|$ meets $\sigma_1, \sigma_2, \sigma_3$, in the planes π_1, π_2, π_3, respectively. These planes meet in pairs in the points $\pi_{12}, \pi_{13}, \pi_{23}$ which determine a plane π_{123} meeting each π_i in a line. π_{123} also meets σ_4 in a line and σ_5 and σ_6, each in a point. The plane π_{123} therefore lies on both V_5 and V_6. As the S_4 describes the pencil, the plane π_{123} describes the cubic variety

$$\frac{x_1}{x_2} = \frac{(a_3b_2)x_3 + (a_4b_2)x_4}{(a_1b_3)x_3 - (a_4b_1)x_4} = \frac{(a_5b_2)x_5 + (a_6b_2)x_6}{(a_1b_5)x_5 - (a_6b_1)x_6}.$$

5. *Transformations in S_n Defined by n Bilinear Equations.* The n bilinear equations

$$A_r \equiv \sum_{i=1}^{n+1}\sum_{k=1}^{n+1} a_{ik}^{(r)} x_i x_k' = 0, \quad (r = 1, 2, \cdots, n)$$

define each x_i' as a function of (x), expressed as a determinant of order r, each element being linear. These determinants belong to a matrix $\|a_{ik}^{(r)}\|$ of n rows and $n+1$ columns. They are satisfied by a manifold M of order $(n+1)n/2$ and of dimensionality $n-2$. Thus, for $n=3$, there results a C_6, defining a web of cubic surfaces. Conversely, the system of primals of order n containing M form a homaloidal system.

An S_{n-k}, defined by k primes in (x'), is transformed into a variety of order $n(n-1)\cdots(n-k+1)/k!$ and of dimensionality $n-k$, having in common with M a variety of order $k \cdot {}_nC_{k+1} \cdot (n+1)/(n-k)$ and of dimensionality $n-k-1$.

Thus, if $n=3$, $k=2$, a line of (x') is transformed into a space cubic curve meeting C_6 in eight points. The lines meeting M in n points generate a primal of order n^2-1. No line has $n+1$ points on M apart from the generators.*

* L. Godeaux, Istituto Lombardo Rendiconti, vol. 43 (1910), pp. 116–119.

In addition to the order $(n+1)n/2$ of M the orders of the double, triple, and other multiple manifolds on this given variety M can be expressed by equating to zero all the determinants of order n, $n-1$, $\cdots$, respectively. The hth variety of this system exists if $d-h(d-n+h)\geqq 0$, d being the dimensionality of the space, and this is its dimension. Its order is given by

$$\frac{(d+n-2q)_h(d+n-2q+1)_h\cdots(d+n-q)_h}{(h)_h(h+1)_h\cdots(n)_h},$$

where $n-h=q$;* $(k)_h$ represents the number of combinations of k things, taken h at a time.

6. *Maps of S_1, S_2, $\cdots$ in a General (n, n) of Veneroni Type.* (a) If the point x describes a straight line, the image x' describes a normal C_n of S_n', as is seen by solving the equations of the line for every x_i in terms of two homogeneous ones, and then regarding these as the parameters in the locus of x'. The curve may also be defined as the locus of intersections of corresponding primes of $n-1$ projective pencils of primes.

(b) If the point x describes a plane, from its equations all the coordinates x_i can be eliminated except three, which appear linearly and homogeneously. The n defining bilinear equations can be interpreted as n projective systems of $|S_{n-1}|$, each having an S_{n-3} for base.

For example, if the coordinates remaining in (x) are replaced by λ, μ, ν, there are n projective systems $\lambda p^{(i)}+\mu q^{(i)}+\nu r^{(i)}=0$, $p^{(i)}=0$, $q^{(i)}=0$, and $r^{(i)}=0$ being the equations of primes in (x') for $i=1, 2, \cdots, n$. Each S_{n-1} defined by one of these equations passes through $p^{(i)}=0$, $q^{(i)}=0$, and $r^{(i)}=0$, hence through an S_{n-3}. By eliminating λ, μ, ν there results a matrix of three rows and n columns, each element being linear in x_i'. The locus common to all these is a surface F_2 of order $n(n-1)/2$. Each x_i' is a rational polynomial of order n in λ, μ, ν. Since a variable double point can not exist in a linear system of plane curves by Bertini's theorem, the intersections of F_2 and each surface S_{n-1} are represented by plane curves of order n with simple base points. Hence F_2 contains $n(n+1)/2$ lines, and the intersection of F_2 and any S_{n-1} is of genus $(n-1)(n-2)/2$.

* C. Segre, Roma, Reale Accademia dei Lincei, Rendiconti, (5), vol. 9_2 (1900), pp. 253–260.

The $n(n+1)/2$ lines on F_2 are the images of the points in which a plane in (x') meets the $n+1$ base $[n-2]$-spaces σ_i' and of those in which it meets the ruled manifold $R'^{(n+1)(n-2)/2}_{n-2}$. The images of the first set of points are the lines meeting n of the base σ_i and the images of the second set are the generators of $R^{(n+1)(n-2)/2}_{n-2}$.

Each surface F_2 of the system meets the ruled manifold $R^{(n+1)(n-2)/2}_{n-2}$ in $(n+1)(n-2)/2$ lines and contains $n+1$ other lines.

Hence the ∞^n sections of the F_2 of the system are mapped upon a plane by the system of curves of order n through $n(n+1)/2$ points.

For an arbitrary plane, the lines on the image surface F_2 are mutually skew. A line in the image (λ, μ, ν) plane is the image of a normal curve C_n of order n in S_n. If the image line passes through a base point, the C_n consists of a normal C_{n-1} of order $n-1$ in S_{n-1} and one of the $n(n+1)/2$ lines intersecting it in one point. The residual section in the S_{n-1} is a curve $C_{n(n-3)/2}$ of order $n(n-3)/2$ having for an image in the (λ, μ, ν) plane a C'_{n-1} through the other $n(n-1)/2$ points; it is of genus $(n-2)(n-3)/2$. Through this $C_{n(n-3)/2}$ there pass ∞^1 primes, each containing a C_{n-1}, hence the $C_{n(n-3)/2}$ lies in an $[n-2]$-dimensional space S_{n-2}, and each S_{n-1} through it meets F_2 in a C_{n-1} which intersects the line not secant to $C_{n(n-3)/2}$ and also the latter curve in $n-1$ points.

Among the lines of the pencil A_i, images of curves C_{n-1} on F_2, there is one through another base point A_k. The curve on the surface F_2 having this line for image consists of two base lines and a curve C_{n-2} of order $n-2$, hence lying in an S_{n-2}. Since the residual plane curve passes through A_k and the composite curve is the image of a prime section of F_2, it follows that the residual curve on F_2 is tangent to the S_{n-2} passing through $n-1$ curves C_{n-2}, and the space of each C_{n-2} is tangent to two residual curves. This residual curve $C_{(n^2-3n+2/4)}$ of order $(n^2-3n+4)/2$ and of genus $(n-3)(n-4)/2$ intersects C_{n-2} in $n-2$ points. There are therefore $n(n-1)/2$ curves C_{n-2} of S_{n-2} lying on F_2, intersecting in pairs in not more than one point; if their image lines meet in the same base points, the associated C_{n-2} do not intersect. The curves $C_{(n^2-3n+4)/2}$ intersect in pairs in $(n-2)(n-3)/2$ points apart from the base points.

Any two F_2 of the system do not have any points in common. The surfaces F_2 do not contain rational curves of order less than $n-2$, apart from the base lines.

For $n=4$, an S_3 meets every pencil of the quartic primals $|\psi_4|$ in a pencil of quartic surfaces, each containing the intersection of the basic two-dimensional surface F_2 of order six and S_3, a curve C_6 of order six and of genus three. Hence each quartic surface is invariant under an infinite discontinuous group of Cremona transformations.*

Similarly, for $n=5$, an S_4 meets a net of quintic primals in a net of quintic surfaces, each passing through the intersection of the basic two-dimensional surface F_2 of order ten (that is, in ten points) and an S_4, a curve C_{10} of order ten and of genus six. An S_4 containing a normal C_4 on F_2 meets it in a residual C_6 of order six and of genus three, which intersects C_4 in four points. But through this residual C_6 pass ∞^1 $|S_4|$, each meeting F_2 in a normal C_4 of S_4; hence the C_6 lies in the base of the pencil $|S_4|$, and the quartic surfaces through it have the same property as that mentioned in the case $n=4$.

This property is true for prime sections of pencils of primals in S_n, since their equations can always be written in determinantal form.

Any S_{n-2} through one of the bases, for example, $p=q=r=0$, meets each homologous S_{n-2} of the other projective systems in $n-1$ spaces S_{n-4}. The pencil of $|S_{n-1}|$ through the homologous S_{n-2} of the base $p=q=r=0$ meets the base in a pencil $|S_{n-3}|$. Similarly for each of the other systems. There are then in the arbitrary S_{n-2} through the base $n-1$ spaces S_{n-4}, axes of projective pencils of $|S_{n-3}|$, each of the form $a+\lambda b=0$. The condition that these $n-1$ spaces are concurrent is expressed by an equation of order $n-1$ in λ. Hence in the given S_{n-2} there are $n-1$ variable points of F_2. Since an S_{n-2} meets F_2 in $(n+1)n/2$ points, it follows that *each base meets F_2 in $(n-1)(n-2)/2$ points in addition to a base curve.*

(c) If (x) describes an S_3, the equations may be written in the form $x_i' = f_i(\lambda, \mu, \nu, \rho)$, each f_i being a polynomial of order n. These three-dimensional varieties are presented by their prime sections, which are expressed in terms of surfaces of order n, all passing through a surface of order $(n-3)\cdot {}_nC_3\cdot(n+1)/3$.

* Snyder and Sharpe, Transactions of this Society, vol. 16 (1915), pp. 62–70.

If the $n+1$ projective systems of lines, planes, $\cdots$, primes with point vertices $A_0, \cdots, A_n$, are considered arbitrarily in S_n, the locus of intersections of corresponding primes of the system is a variety M of order $(n+1)n/2$ and of dimensionality $n-2$. The locus of intersections of corresponding primes of n of the systems, omitting A_0, is a determinantal primal of order n, Φ_0, passing through all the vertices of the system except A_0 and containing M. In the same way primals Φ_i are obtained, $(i=1, 2, \cdots, n)$, each containing M and all the vertices except A_i. The $n+1$ primals are linearly independent.

Similarly, for the loci of intersections of corresponding primes of $n-1, n-2, \cdots, 3, 2$ of the systems.

The synthetic argument made by Todd* for $n=4$ can be extensively generalized to apply for n general. There are n degrees of freedom to account for the ∞^n primes of S_n. There is a base curve of order $(n+1)n/2$, the intersection of a manifold M of order $(n+1)n/2$ and an S_3. The genus of this curve is determined by the postulation. A surface of order n meets a curve of order m and of genus p in $mn-p+1$ points in order to pass through the curve. The postulation of the surface is $[(n+3)(n+2)(n+1)/6]-1-n$, hence

$$\frac{n^2(n+1)}{2} - p + 1 = \frac{(n+3)(n+2)(n+1)}{6} - 1 - n,$$

from which $p=(n-1)(n-2)(2n+3)/6$. *The projective systems of primes through the three spaces S_3' as bases generate a three-dimensional rational variety of S_n mapped on S_3 by means of surfaces of order n passing through a curve of order $(n+1)n/2$ and of genus $(n-1)(n-2)(2n+3)/6$.* These varieties have $(n+1)\ n(n-1)/6$ singular points, mapped by the multisecants of the base curve.

7. *The Base Elements of the Veneroni Transformation.* The $n+1$ base S_{n-2} form part of the base $[n-2]$-dimensional manifold M of order $(n+1)n/2$, defined by the matrix $\|a_{ik}\|$; the residual is a ruled variety R of order $(n+1)(n-2)/2$ formed by the lines which meet all the $n+1$ base S_{n-2}.

* J. A. Todd, Proceedings of the Cambridge Philosophical Society, vol. 26 (1930), pp. 323–333.

Each normal C_n image of a line meets each base S_{n-2} in $n-2$ points and does not intersect the ruled variety.

The images of planes intersect R in $(n+1)(n-2)/2$ lines. The plane meets each base S_{n-2} in a point, the image of which is a line meeting n of the base S'_{n-2} and lying on F_2. Each base S_{n-2} meets R in a manifold of dimensionality $n-3$ and of order $n-1$. For $n=4$, the two-dimensional variety of order 5 has an infinite number of plane elliptic cubic curves, but the corresponding property is not true for larger values of n although the intersections of each base S_{n-2} and R are birationally equivalent.

CORNELL UNIVERSITY AND
WELLS COLLEGE

ON THE CHARACTERISTIC ROOTS OF MATRIC POLYNOMIALS*

BY N. H. McCOY

1. *Introduction.* Unless otherwise stated, all matrices and polynomials are assumed to have coefficients in an arbitrary algebraically closed field K.

Let A and B denote square matrices of order n. If the characteristic roots of every polynomial $f(A, B)$ are all of the form $f(\lambda, \mu)$, where λ and μ are characteristic roots of A and B, respectively, then in accordance with a notation to be introduced below, we shall say that the matrices A, B have property I_n. By a theorem of Frobenius,† the matrices A, B have this property if they are commutative, but this is by no means a necessary condition. The study of pairs of matrices having property I_n has been the subject of papers by Bruton, Ingraham, and Roth.‡ However, in no case have conditions been obtained which are both necessary and sufficient for the existence of this property.

---

* Presented to the Society, October 26, 1935.

† G. Frobenius, *Über vertauschbare Matrizen*, Sitzungsberichte der Preussischen Akademie der Wissenschaften zu Berlin, 1896, pp. 601–614.

‡ The papers by Bruton and by Ingraham have not yet been published in full but abstracts are available as follows: G. S. Bruton, *Certain aspects of the theory of equations for a pair of matrices*, this Bulletin, vol. 38 (1932), p. 633; M. H. Ingraham, *A study of certain related pairs of square matrices*, this Bulletin, vol. 38 (1932), pp. 633–634. Roth's paper is *On the characteristic values of the matrix* $f(A, B)$, Transactions of this Society, vol. 39 (1936), pp. 234–243.

If there exists a non-singular matrix T such that $T^{-1}AT$, $T^{-1}BT$ are both in triangle form,* we may say that A and B have property II_n. Williamson† has studied the problem of determining conditions under which the matrices A, B have property II_n and in particular has shown that if A is non-derogatory, then property I_n implies the existence of property II_n, and conversely. Under the same hypothesis on A, he has also exhibited other necessary and sufficient conditions for the existence of property II_n.

In §2 of the present paper we shall introduce and solve a problem somewhat more general than either of those mentioned above. As a special case we shall exhibit necessary and sufficient conditions for any finite set of matrices to have property I_n or II_n. In particular, it will appear that these two properties are always equivalent. Another special case yields a perfection of Frobenius' theorem, which for the case of two matrices may be stated as follows.

A necessary and sufficient condition that the matrices A, B have property I_n is that for every polynomial $h(A, B)$, the matrix

$$h(A, B)(AB - BA)$$

be nilpotent.‡

The condition of this theorem is clearly satisfied if A and B are commutative or quasi-commutative.§ We shall give, in §3, a direct proof of this theorem without use of the representation theory introduced in §2.

Finally, in §4, we point out the connection of the present paper with the theory of Lie algebras. If the field K has characteristic 0, the equivalence of properties I_n and II_n is seen to be an almost immediate consequence of known theorems on Lie algebras.

---

* That is, all elements below the principal diagonal are zero.

† J. Williamson, *The simultaneous reduction of two matrices to triangle form*, American Journal of Mathematics, vol. 57 (1935), pp. 281–293.

‡ See Williamson, loc. cit., p. 292.

§ The matrices A, B are quasi-commutative if $AB-BA$ is not zero but is commutative with both A and B. It follows that $AB-BA$ is necessarily nilpotent. See a previous paper, *On quasi-commutative matrices*, Transactions of this Society, vol. 36 (1934), pp. 327–340.

2. *The General Theorem.* Let A_i, $(i=1, 2, \cdots, m)$, be given matrices of order n, and denote by P the algebra of polynomials in these matrices. The elements of P then form a representation of the algebra P.* Hence it is known that all elements of P may, by a similarity transformation, be simultaneously reduced to the form

$$(1) \qquad \left\| \begin{matrix} B_{11} & B_{12} \cdots B_{1l} \\ 0 & B_{22} \cdots B_{2l} \\ \cdot & \cdot \cdot \cdot \cdot \cdot \cdot \\ 0 & 0 \cdots B_{ll} \end{matrix} \right\|,$$

where the set $P^{(k)}$ of square matrices B_{kk}, $(k=1, 2, \cdots, l)$, is an irreducible representation of P. These irreducible components $P^{(k)}$ of P are uniquely determined to within a similarity transformation and thus their orders are completely determined. The fact that $P^{(k)}$ is an irreducible representation of P means essentially that $P^{(k)}$ is a simple algebra, that is, one with no proper invariant sub-algebra. We shall assume henceforth, as we may without loss of generality, that all elements of P are in the form (1).

Let Q denote the minimum invariant sub-algebra of P containing all the elements

$$A_iA_j - A_jA_i, \qquad (i, j = 1, 2, \cdots, m;\ i \neq j).$$

If now C_i, $(i=1, 2, \cdots, s)$, is a basis of Q, the general element of Q may be written in the form

$$(2) \qquad Q_x = x_1C_1 + x_2C_2 + \cdots + x_sC_s,$$

where the x_i are indeterminate elements of K. If $Q=0$, we shall write $Q_x \equiv 0$. The characteristic polynomial $|Q_x - \lambda|$ of Q_x may be called the *characteristic polynomial of* Q.

Let r denote a fixed integer, $0 \leqq r \leqq n$. We now define the following three properties:

(I_r). At least r of the characteristic roots of every polynomial $f(A_1, A_2, \cdots, A_m)$ are of the form $f(\lambda_1, \lambda_2, \cdots, \lambda_m)$, where λ_i

* For proofs of the fundamental theorems on representations of algebras, see E. Noether, *Hyperkomplexe Grössen und Darstellungstheorie*, Mathematische Zeitschrift, vol. 30 (1929), pp. 641–692.

is a characteristic root of A_i, $(i=1, 2, \cdots, m)$, but some polynomial has not more than r characteristic roots of this form.

(II_r). Exactly r of the irreducible components $P^{(k)}$ of P are of order 1.

(III_r). The characteristic polynomial of Q is divisible by λ^r but not by λ^{r+2}.

The principal result of this paper is the following theorem.

THEOREM 1. *The properties* I_r, II_r, *and* III_r *are equivalent*, $(r=0, 1, \cdots, n)$.

The proof of this theorem will be made to depend upon several lemmas which we proceed to establish.

LEMMA 1. $\mathrm{I}_r \supset \mathrm{III}_{r_1 \geqq r}$.*

This is almost obvious. For each element of Q may be expressed as a finite sum of terms of the form $g(A_iA_j-A_jA_i)h$, where g and h are polynomials in the A_i. Hence I_r implies that every element of Q has at least r zero characteristic roots. This is equivalent to property $\mathrm{III}_{r_1 \geqq r}$. For if

$$|Q_x - \lambda| \equiv (-1)^n\lambda^n + \phi_1(x)\lambda^{n-1} + \cdots + \phi_n(x),$$

and every element of Q has at least r zero characteristic roots, it follows that the polynomials $\phi_{n-r+1}(x), \cdots, \phi_n(x)$ vanish for all choices of the x_i in K. And since K has an infinite number of elements, it is clear that all the coefficients in these polynomials are zero, and thus $|Q_x-\lambda|$ is divisible by λ^r.

LEMMA 2. $\mathrm{II}_r \supset \mathrm{I}_{r_2 \geqq r}$.

Suppose $A_i \rightarrow A_i^{(k)}$ by the correspondence $P \rightarrow P^{(k)}$. If $f(A_1, A_2, \cdots, A_m)$ is any polynomial, it follows from the form (1) of all matrices involved that the characteristic roots of $f(A_1, A_2, \cdots, A_m)$ are precisely the characteristic roots of all the matrices $f(A_1^{(k)}, A_2^{(k)}, \cdots, A_m^{(k)})$, $(k=1, 2, \cdots, l)$. If now $P^{(k)}$ is of order 1, then $A_i^{(k)}$ is a scalar and hence a characteristic root of A_i, $(i=1, 2, \cdots, m)$. In this case $f(A_1^{(k)}, A_2^{(k)}, \cdots, A_m^{(k)})$ is a characteristic root of $f(A_1, A_2, \cdots, A_m)$. Thus, if r of the $P^{(k)}$ are of order 1, at least r of the characteristic roots will be of the prescribed form, which is property $\mathrm{I}_{r_2 \geqq r}$.

* By this notation we mean that property I_r implies the existence of property III_{r_1} for some $r_1 \geqq r$.

By the homomorphic correspondence $P \rightarrow P^{(k)}$, suppose that $Q \rightarrow Q^{(k)}$. Then $Q^{(k)}$ is an invariant sub-algebra of $P^{(k)}$, and since $P^{(k)}$ is simple, must therefore be zero or $P^{(k)}$ itself. We shall now prove the following lemma.

LEMMA 3. *$P^{(k)}$ is of order 1 if and only if $Q^{(k)} = 0$, $(k = 1, 2, \cdots, l)$.*

Now $Q^{(k)}$ clearly contains the matrices $A_i^{(k)} A_j^{(k)} - A_j^{(k)} A_i^{(k)}$, $(i, j = 1, 2, \cdots, m)$. But $P^{(k)}$ is an algebra of polynomials in the matrices $A_i^{(k)}$, $(i = 1, 2, \cdots, m)$, with coefficients in K, and thus $P^{(k)}$ is commutative if $Q^{(k)} = 0$. In this case $P^{(k)}$ is a representation of a commutative algebra, irreducible in an algebraically closed field. It therefore follows that $P^{(k)}$ is of order 1.* If, on the other hand, $P^{(k)}$ is of order 1, it is obvious that multiplication is commutative, and, since each element of $Q^{(k)}$ is a finite sum of terms of the form $g^{(k)}(A_i^{(k)} A_j^{(k)} - A_j^{(k)} A_i^{(k)})h^{(k)}$, where $g^{(k)}$ and $h^{(k)}$ are polynomials in the $A_i^{(k)}$, it follows that $Q^{(k)} = 0$.

We may now establish the following lemma.

LEMMA 4. $\text{III}_r \supset \text{II}_r$.

Let us first consider the case in which $r = n$, and assume the presence of property III_n. This means that all elements of Q are nilpotent, that is, Q is contained in the radical† of P. Then $Q^{(k)}$ is contained in the radical of $P^{(k)}$ and, since $P^{(k)}$ has a unit element, we must have $Q^{(k)} = 0$, $(k = 1, 2, \cdots, l)$. From the preceding lemma it follows that all $P^{(k)}$, $(k = 1, 2, \cdots, l)$, are of order 1, and hence $l = n$. Thus $\text{III}_n \supset \text{II}_n$.

Now suppose the matrices A_i have property III_r, where $r < n$, and thus $Q \neq 0$. By the correspondence $P \rightarrow P^{(k)}$, let $C_i \rightarrow C_i^{(k)}$, $(i = 1, 2, \cdots, s)$. Then from (2) it follows that $Q_x \rightarrow Q_x^{(k)}$, where

$$Q_x^{(k)} = x_1 C_1^{(k)} + x_2 C_2^{(k)} + \cdots + x_s C_s^{(k)}. \tag{3}$$

Now by a proper choice of the x_i any element of $Q^{(k)}$ can be expressed in the form (3), and hence $Q^{(k)} = 0$, if and only if $Q_x^{(k)} \equiv 0$. We shall conclude the proof of the lemma by showing that precisely r of the $Q_x^{(k)}$, $(k = 1, 2, \cdots, l)$, vanish identically.

From the form (1) of all our matrices, it is clear that

$$|Q_x - \lambda| \equiv \prod_{k=1}^{l} |Q_x^{(k)} - \lambda|.$$

* See E. Noether, loc. cit., p. 683.

† Maximum nilpotent invariant sub-algebra.

Suppose that exactly t of the $Q_x^{(k)}$ are zero. Then we have

$$|Q_x - \lambda| \equiv (-1)^t \lambda^t \prod |Q_x^{(j)} - \lambda|,$$

where j takes only those values for which $Q_x^{(j)} \not\equiv 0$, and thus $Q^{(j)} = P^{(j)}$. Hence, by the hypothesis of property III_r, we have $t \leqq r$. If $t < r$, then $\prod |Q_x^{(j)} - \lambda|$ must be divisible by λ, and thus $\prod |Q_x^{(j)}| \equiv 0$. Hence for some j, $|Q_x^{(j)}| \equiv 0$. But this is impossible as $Q^{(j)} = P^{(j)}$ has a unit element, and not all elements can be singular. We must therefore have $t = r$. By Lemma 3, it follows that precisely r of the $P^{(k)}$ are of order 1, and the present lemma is established.

The proof of the theorem now follows readily by formal logic. For from Lemmas 1, 2, and 4, we have

$$\mathrm{II}_r \supset \mathrm{I}_{r_2 \geqq r} \supset \mathrm{III}_{r_1 \geqq r_2} \supset \mathrm{II}_{r_1},$$

and

$$\mathrm{I}_r \supset \mathrm{III}_{r_1 \geqq r} \supset \mathrm{II}_{r_1} \supset \mathrm{I}_{r_2 \geqq r_1}.$$

In both cases we must have $r = r_1 = r_2$, and the equivalence of the three properties I_r, II_r, and III_r is at once obvious. The theorem is therefore established.

From the equivalence of properties I_r and II_r we may obtain at once the following corollary.

COROLLARY. *Let the characteristic roots of A_i be λ_{ij}, $(i = 1, 2, \cdots, m; j = 1, 2, \cdots, n)$. If the matrices A_i have property I_r, it is possible to order these roots in such a way that r of the characteristic roots of an arbitrary polynomial $f(A_1, A_2, \cdots, A_m)$ are $f(\lambda_{1j}, \lambda_{2j}, \cdots, \lambda_{mj})$, $(j = 1, 2, \cdots, r)$.*

3. *The Special Case $r = n$.* The equivalence of properties I_n and III_n is seen to be a direct generalization of Frobenius' theorem on the characteristic roots of polynomials in commutative matrices. In the present section we shall give a direct proof of the equivalence of these two properties without introduction of property II_n. If we let N denote the radical of the ring P, the theorem to be proved may be restated as follows.

THEOREM 2. *A necessary and sufficient condition that the matrices A_i, $(i = 1, 2, \cdots, m)$, have property I_n is that the quotient ring* P/N be commutative.*

* The term "quotient ring" will be used for the German "Restklassenring." With this exception, the notation and terminology of this section will follow as closely as possible that of van der Waerden, *Moderne Algebra*, 1930 and 1931.

The necessity of the condition is almost obvious. For property I_n implies at once that each matrix $f(A_iA_j - A_jA_i)g$, where f and g are arbitrary elements of P, is nilpotent. Hence

$$A_iA_j - A_jA_i \equiv 0 \quad (N), \qquad (i, j = 1, 2, \cdots, m).$$

We now assume that P/N is commutative, and shall show that the matrices A_i have property I_n. By the homomorphic correspondence $P \rightarrow P/N$, suppose $A_i \rightarrow \overline{A}_i$, $(i=1, 2, \cdots, m)$. The elements of K^* go over into elements of a field simply isomorphic to K, which we shall not distinguish from K itself. Then

$$f(A_1, A_2, \cdots, A_m) \rightarrow f(\overline{A}_1, \overline{A}_2, \cdots, \overline{A}_m). \tag{4}$$

Now let $x_1, x_2, \cdots, x_m$ be commutative indeterminates and consider the ring $K[x] = K[x_1, x_2, \cdots, x_m]$ of polynomials in the x_i. Since, by hypothesis, $\overline{A}_i\overline{A}_j = \overline{A}_j\overline{A}_i$, it follows that the correspondence

$$g(x_1, x_2, \cdots, x_m) \rightarrow g(\overline{A}_1, \overline{A}_2, \cdots, \overline{A}_m) \tag{5}$$

is a ring homomorphism between $K[x]$ and P/N. Hence

$$P/N \cong K[x]/M, \tag{6}$$

where M is the ideal of elements $h(x_1, x_2, \cdots, x_m)$ in $K[x]$ such that $h(\overline{A}_1, \overline{A}_2, \cdots, \overline{A}_m) = 0$.†

Let the minimum function of A_i be $\phi_i(\lambda)$. Then $\phi_i(A_i) = 0 = \phi_i(\overline{A}_i)$, and thus $\phi_i(x_i) \equiv 0(M)$. If $\psi_i(x_i)$ denotes the polynomial of minimum degree in x_i alone which belongs to M, then $\phi_i(x_i) \equiv 0(\psi_i(x_i))$. But $\psi_i(\overline{A}_i) = 0$, $\psi_i(A_i) \equiv 0(N)$, and thus $(\psi_i(A_i))^p = 0$. It follows that $[\psi_i(x_i)]^p \equiv 0(\phi_i(x_i))$. Thus the roots of $\psi_i(\lambda) = 0$ are precisely the roots of $\phi_i(\lambda) = 0$.

By a familiar theorem,‡ the ideal M may be expressed in the form

$$M = [M_1, M_2, \cdots, M_k], \tag{7}$$

where the M_i are primary ideals. Their manifolds thus consist of single points, which together form the manifold of M. Suppose the manifold of M_i is $(\lambda_i^{(i)}, \lambda_2^{(i)}, \cdots, \lambda_m^{(i)})$, $(i=1, 2, \cdots, k)$.

* That is the elements of $K \cdot I$, where I is the unit element of P.

† See van der Waerden, op. cit., vol. 1, p. 57.

‡ See van der Waerden, op. cit., vol. 2, p. 37. See also pp. 51–52, and p. 63.

Then by the preceding paragraph, $\lambda_j^{(i)}$ must be a characteristic root of A_j, $(j=1, 2, \cdots, m; i=1, 2, \cdots, k)$.

Now each linear expression $x_j-\lambda_j^{(i)}$, $(j=1, 2, \cdots, m)$, vanishes at the point $(\lambda_1^{(i)}, \lambda_2^{(i)}, \cdots, \lambda_m^{(i)})$, and thus by Hilbert's theorem, some finite power of each of these expressions belongs to M_i. If now $f(x_1, x_2, \cdots, x_m)$ is any element of $K[x]$, and we expand by Taylor's theorem in powers of $x_j-\lambda_j^{(i)}$, $(j=1, 2, \cdots, m)$, it follows that

$$f(x_1, x_2, \cdots, x_m) = f(\lambda_1^{(i)}, \lambda_2^{(i)}, \cdots, \lambda_m^{(i)}) + f_i,$$

where some finite power of f_i belongs to M_i. Let $\alpha(\lambda)$ denote the polynomial

$$\prod_{i=1}^{k} [\lambda - f(\lambda_1^{(i)}, \lambda_2^{(i)}, \cdots, \lambda_m^{(i)})]. \tag{8}$$

Then for sufficiently large ρ, it follows from (7) that

$$\{\alpha[f(x_1, x_2, \cdots, x_m)]\}^{\rho} \equiv 0 \quad (M). \tag{9}$$

Now let $f(A_1, A_2, \cdots, A_m)$ be any element of P, $f(\overline{A}_1, \overline{A}_2, \cdots, \overline{A}_m)$ the corresponding element of P/N. Then $f(x_1, x_2, \cdots, x_m)$ is an element of $K[x]$ which corresponds to $f(\overline{A}_1, \overline{A}_2, \cdots, \overline{A}_m)$ by (5). If $\alpha(\lambda)$ is defined by (8), it then follows from (9) that

$$\{\alpha[f(\overline{A}_1, \overline{A}_2, \cdots, \overline{A}_m)]\}^{\rho} = 0,$$

and thus

$$\{\alpha[f(A_1, A_2, \cdots, A_m)]\}^{\rho l} = 0.$$

The distinct characteristic roots of $f(A_1, A_2, \cdots, A_m)$ are therefore included among the distinct roots of the equation $\alpha(\lambda)=0$, and these are all of the form $f(\lambda_1^{(i)}, \lambda_2^{(i)}, \cdots, \lambda_m^{(i)})$, where $\lambda_j^{(i)}$ is a characteristic root of A_j. The theorem is therefore established.

4. *Connection with Lie Algebras.* The use of the commutator matrices $A_iA_j-A_jA_i$ suggests a connection with the theory of Lie algebras. As a matter of fact, if K has characteristic 0, we can show almost at once that property II_n is a consequence of property III_n, by using known theorems on Lie algebras.

We shall conclude with a brief statement of some facts from this point of view.*

We now assume that the field K has characteristic 0.† A *Lie algebra* of matrices over K is a linear space L which is closed under the commutator operation, $[A, B]=AB-BA$, where A and B are any elements of L. The linear space generated by the commutators of L is itself a Lie algebra, called the first derived algebra of L, and denoted by $L'=[L, L]$. Then $L^{(2)}=[L', L']$, and so on. If there exists an integer s such that $L^{(s)}=0$, then L is said to be *solvable*. The nth power of L may be defined by induction as $L^n=[L, L^{n-1}]$. If, for some finite n, $L^n=0$, L is said to be *nilpotent*. Evidently L is solvable if it is nilpotent.

Now let A_i, $(i=1, 2, \cdots, m)$, be given matrices of order n, and close the linear space generated by the A_i with respect to the commutator operation, thus leading to a Lie algebra *defined* by the A_i. The elements of L' are all of the form $fg-gf$, where f and g are polynomials in the A_i. But in the notation of §2, multiplication is commutative mod Q, and thus all elements of L' belong to Q. Hence under hypothesis III_n, all elements of L' have λ^n as characteristic function. It then follows by a generalization of Engel's theorem that L' is nilpotent. Hence L is solvable and by Lie's theorem all elements of L may be simultaneously transformed to triangle form, which is property II_n.

These considerations enable us to state the following theorem.‡

THEOREM 3. *If the underlying field K has characteristic 0, a necessary and sufficient condition that the matrices A_i, $(i=1, 2, \cdots, m)$, have property I_n is that the Lie algebra L defined by these matrices be solvable.*

SMITH COLLEGE

---

* For proofs and references, see N. Jacobson, *Rational methods in the theory of Lie algebras*, Annals of Mathematics, vol. 36 (1935), pp. 875–885.

† Jacobson has pointed out to me that the Lie theorem does not hold for Lie algebras over a field of characteristic p. Hence this is a necessary restriction.

‡ In this connection see a paper by W. E. Roth, *On k-commutative matrices*, Abstract No. 40-11-349. Roth considered a weaker condition than that L' be nilpotent, and discussed some of its consequences.